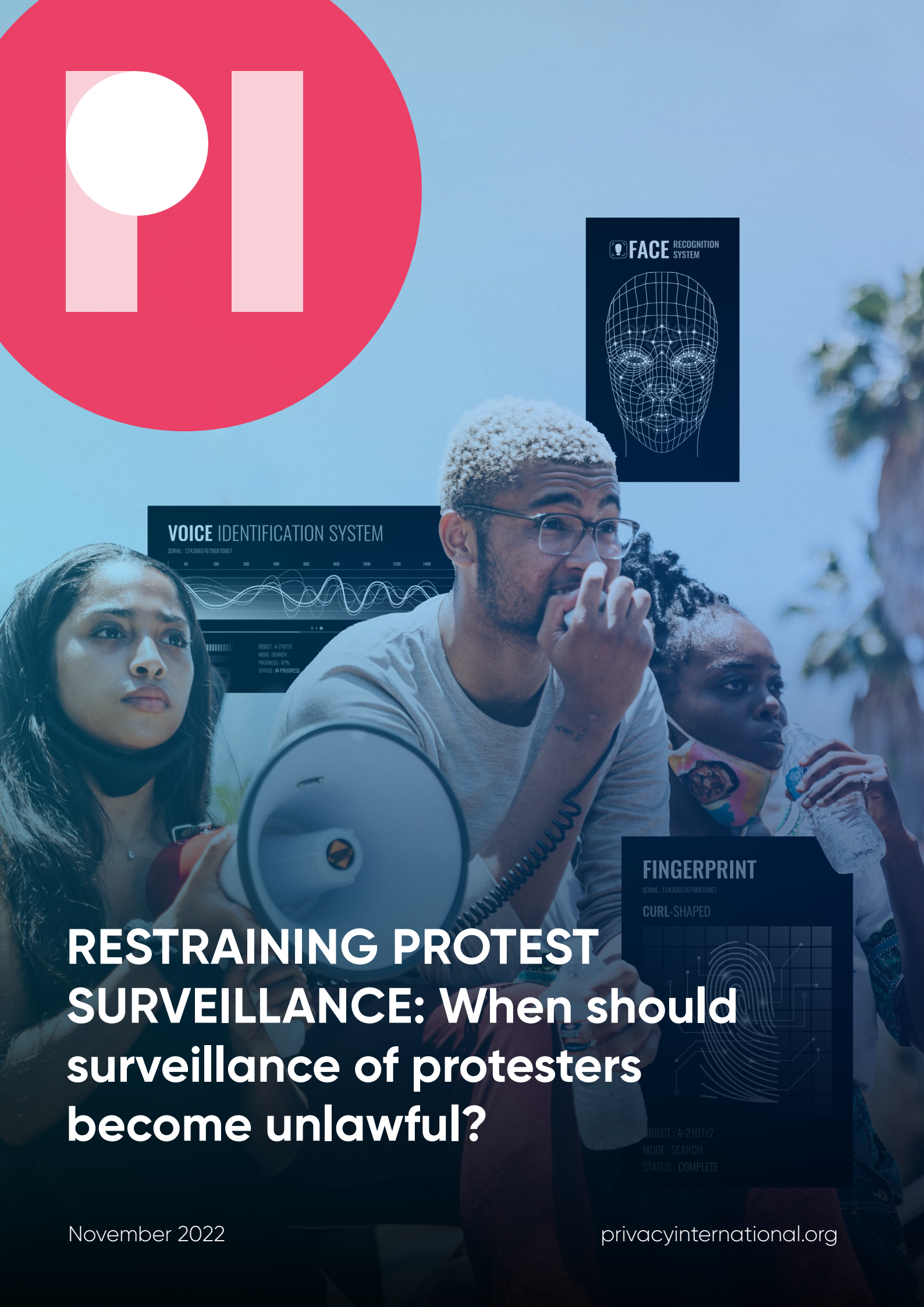


RESTRAINING PROTEST SURVEILLANCE: When should surveillance of protesters become unlawful?

November 2022

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

creative commons

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by Nathan Dumlao on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

RESTRAINING PROTEST SURVEILLANCE:

When should surveillance of protesters become unlawful?

November 2022

CONTENTS

I. INTRODUCTION 1

WHAT CONSTITUTES PARTICIPATION IN A PROTEST? 2

II. PROTEST SURVEILLANCE AND THE RIGHT TO PRIVACY 4

WHAT IS PROTEST SURVEILLANCE? 4

THE RIGHT TO PRIVACY: THE STARTING POINT FOR LEGAL LIMITS ON PROTEST SURVEILLANCE 7

III. THE RIGHT TO FREEDOM OF ASSEMBLY: STRENGTHENING THE LIMITS ON PROTEST SURVEILLANCE 14

HOW DOES PROTEST SURVEILLANCE INTERFERE WITH THE RIGHT TO FREEDOM OF ASSEMBLY? 16

IV. HUMAN RIGHTS STANDARDS FOR RESTRAINING PROTEST SURVEILLANCE 20

V. THE TIMELINE OF A PROTEST: MAPPING INTERFERENCES AND SAFEGUARDS AT EVERY STAGE OF A PROTEST 23

BEFORE A PROTEST: ORGANISING, PLANNING, ASSOCIATING 24

Examples of surveillance deployed before a protest 21

Applying the legal standards 28

DURING A PROTEST: ATTENDING A PROTEST 31

Examples of surveillance deployed during a protest 34

Applying the legal standards 38

AFTER A PROTEST: WHAT HAPPENS TO PROTESTERS' DATA AFTER THEY HAVE PARTICIPATED IN PROTEST? 41

Examples of surveillance deployed after a protest 43

Applying the legal standards 46

VI. CONCLUSION 50

I. INTRODUCTION

What **legal limits should apply to police surveillance** when we are exercising our rights to freedom of assembly, association, and expression through protest?

When, and in what circumstances should **protest surveillance become unlawful?**

> Protest surveillance must be subjected to robust legal constraints in order to protect the fundamental right to privacy and, crucially, freedom of assembly.

Across multiple jurisdictions where PI has worked alongside our international partners, we have documented a lack of human rights-based legal safeguards which effectively restrain surveillance of protests and protest movements. This poses a serious threat to our fundamental human rights, civil liberties, and freedom to dissent.

This paper advocates for specific legal standards and limitations that must apply to surveillance undertaken by law enforcement at every stage of a protest. It also explains why these limits are necessary. **The standards we rely on build on protections which are already contained within the rights to privacy and freedom of assembly under international human rights law.**

- In the section below (section II), we briefly outline how the right to privacy places limits on protest surveillance. We highlight key cases from the jurisprudence from the European Court of Human Rights (ECtHR) and resolutions, guidance, and general comments issued by UN bodies.
- In section III, we then focus on the right to freedom of assembly and how it can be used to impose limits on police surveillance at protests and against protest movements.
- In section IV, we present human rights-based standards that strike the appropriate balance between the police powers to use surveillance at protests and the need to protect our fundamental human rights.
- Finally, section V maps out the 'timeline' of a protest in order to illustrate exactly how protest surveillance interferes with our human rights. This section also explains how the standards we present in section IV can be applied in practice at every stage of a protest.

WHAT CONSTITUTES PARTICIPATION IN A PROTEST?

While it is difficult to outline the defining characteristics of a protest, international human rights standards which protect freedom of assembly, association, and expression, generally include the key 'sites of dissent' in which the act(s) of thinking, dissenting, organising, and assembling take place and amount to participation in protest or contribution to major social movements.

Article 20 of the Universal Declaration of Human Rights (UDHR), and Articles 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR) protect the rights to peaceful assembly and association. The UN Human Rights Committee has framed participation in a peaceful assembly as "organising or taking part in a gathering of persons for a purpose such as expressing oneself, conveying a position on a particular issue or exchanging ideas."[1] While these instruments focus on protecting participation in 'peaceful' assemblies, international human rights law makes it clear that there is a presumption in favour of assuming that assemblies are peaceful,[2] and "isolated acts of violence by some participants should not be attributed to others…or to the assembly as such."[3]

Additionally, the right to participate in and organise assemblies is protected whether it is exercised in person (physically) or online "through the technologies of today, or through technologies that will be invented in the future."[4]

---

1 General Comment No. 37: On the right of peaceful assembly (article 21), 129th Session, adopted 17 September 2020, UN Doc CCPR/C/GC/37, para. 12, accessed online: https://undocs.org/CCPR/C/GC/37.

2 UN Human Rights Council, "Report of the Special Rapporteur on the rights to freedom of assembly and of association", (2013), UN Doc A/HRC/23/39, para. 50, accessed online: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.39_EN.pdf; See also, Venice Commission and OSCE/ODIHR "Guidelines on Freedom of Assembly", (2019), CDL-AD(2019)017, para. 30, accessed online: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2019)017rev-e.

3 n1, General Comment No. 37, at para. 18.

4 UN Human Rights Council, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", (2019), UN Doc A/HRC/41/41, accessed online: https://undocs.org/A/HRC/41/41. For more references to the importance of States' obligations to protect human rights both online and offline see also, UN General Assembly Resolution 73/173 on the Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association, (2019), UN Doc A/RES/73/173, accessed online: https://undocs.org/en/A/RES/73/173; UN Human Rights Council Resolution 38/7 on the Promotion, protection and enjoyment of human rights on the internet, (2018), UN Doc A/HRC/RES/38/7, accessed online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/215/67/PDF/G1821567.pdf?OpenElement

A distinguishing feature of the right to peaceful assembly is its role **"as an enabling right in opening up spaces and opportunities for genuine and effective engagement by civil society actors."**[5]

Finally, while some protests are truly spontaneous eruptions of public discontent, others are organised: by activists, trade unionists, and the general public. Take for example the Gezi Park protests which took place in 2013 in Turkey. Country-wide protests erupted after a small group of activists staged a sit-in at Gezi Park in Istanbul to protest the municipality's plans to demolish the park. Within a week, Turkey witnessed "the largest popular protests in its 90-year history,"[6] as people took to the streets to protest a range of issues, from 'the right to use the city' to democratic rights and individual freedoms.[7]

Although we do not attempt to define 'protest', the fundamental safeguards that we are advocating for should apply to all forms of assemblies – those that include acts of civil disobedience, and those that are physical or virtual and planned or spontaneous.

5 Written submission prepared by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, (2019), accessed online: https://bit.ly/3R3emOH.

6 Gökbörü Sarp Tanyildiz, "The Gezi Protests: The Making of the Next Left Generation in Turkey", in "Protests and Generations: Legacies and Emergences in the Middle East, North Africa and the Mediterranean: 05 (Youth in a Globalizing World)", 2020. See also, Amnesty International, "Gezi Park Protests" (2013), accessed online at: https://www.amnesty.org/en/wp-content/uploads/2021/06/eur440222013en.pdf.

7 Özge Zihnioğlu, "The Legacy of the Gezi Protests in Turkey", Carnegie Europe, 4 October 2019, accessed online at: https://carnegieeurope.eu/2019/10/24/legacy-of-gezi-protests-in-turkey-pub-80142.

II. PROTEST SURVEILLANCE AND THE RIGHT TO PRIVACY

WHAT IS PROTEST SURVEILLANCE?

Using increasingly intrusive technologies, law enforcement and security agencies can monitor, track, collect, analyse, and store information about anyone involved in organising or attending protests. This includes collecting data from protestors' social media accounts, virtual group chats, and online profiles, as well as hacking into devices and cloud-storage accounts. It also includes live collection of biometric data at protests, such as facial data and gait recognition, and data extraction from devices after protesters are detained by law enforcement. Across the world, we are witnessing an alarming rise in law enforcement agencies' use of these technologies to collect highly intrusive personal data about protesters.[8]

The problem is that police forces around the world are using an ever-expanding range of data-gathering/surveillance tools at protests without being subjected to robust legal constraints or limitations on their powers. Together with our international partners, we have highlighted instances where law enforcement agencies either have no lawful basis for deploying certain surveillance technologies at protests,[9] or rely on broad and generic policing powers to deploy technologies[10] which **violate our right to freedom assembly,** and **unlawfully interfere with our right to privacy.** For example, in the UK, the police can process

8 Privacy International's Protest Tracker, accessible online: https://privacyinternational.org/examples/tracking-protest-surveillance; See also, Privacy International, "Protest Surveillance", accessible online: https://privacyinternational.org/learn/protest-surveillance.

9 See, for example, Privacy International, "PI and 30 CSOs unite against the use of live facial recognition technology", 23 August 2021, accessible online: https://privacyinternational.org/advocacy/4616/pi-and-30-csos-unite-against-use-live-facial-recognition-technology; See also, Privacy International, "IMSI Catchers: facilitating indiscriminate surveillance of protesters", 19 June 2020, accessible online: https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters.

10 See, for example, Fundación Karisma, "Guns versus cell phones" 31 October 2021, accessed online: https://web.karisma.org.co/guns-versus-cellphones/; See also, Privacy International and The Defenders Coalition, "Impact of Communication Surveillance on Human Rights Defenders in Kenya", 23 March 2021, accessible online: https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya.

a broad range of personal data collected at protests, provided they are exercising a law enforcement function and such processing is necessary for the administration of justice. There is no requirement that the protest be violent or at risk of becoming violent before data processing can begin. Moreover, the police are not limited to processing data in relation to preventing offences at the protest.[11]

Privacy International (PI) has published guides explaining how police forces in the UK use specific technologies to conduct surveillance at protests and what protesters can do to minimise risks to their privacy. We also worked with partners across Argentina, Colombia, Palestine, and Paraguay to publish guides about how police forces in those countries deploy similar practices and technologies.

Unrestrained protest surveillance means that people will never actually be able to associate or assemble *freely* – that is, free from interference, free from the fear that their actions are being recorded, and free from the fear of retribution or criminalisation for exercising basic freedoms.

Protests are sites of dissent which are fundamental to democratic governance. People must be free to dissent by organising and attending protests without the threat of law enforcement subjecting them to unknown sanctions or interfering with their right to privacy. As has been repeatedly recognised by the ECtHR, "in view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of

11 Privacy International, "Fact sheet on your data rights in relation to police surveillance at protests," 29 June 2021, accessible online: https://privacyinternational.org/long-read/4507/fact-sheet-your-data-rights-relation-police-surveillance-protests#1

democratic processes under the cloak of defending them, [there must be] adequate and effective safeguards against abuse."[12]

This is exacerbated when we consider the reality of the ways in which we protest today. Specifically, how essential digital tools such as the internet, mobile devices and privately-owned social media platforms are to organising, associating, and protesting. The UN Human Rights Committee has highlighted this:

> *The way in which assemblies are conducted and their context changes over time. This may in turn affect how they are approached by the authorities. For example, given that emerging technologies offer the opportunity to assemble either wholly or partly online and often play an integral role in organising, participating in, and monitoring physical gatherings, interference with such communications can impede assemblies [...] Moreover, there is increased private ownership and other forms of control of publicly accessible spaces and communication platforms. Considerations such as these need to inform a contemporary understanding of the legal framework that article 21 requires.*[13]

Throughout this paper, when we refer to "protest surveillance" we mean any type of overt[14] or covert[15] information and/or intelligence gathering which includes the processing, such as collection, analysis, use, and retention of personal data about individuals who are exercising their right to protest, before, during, and after a protest, regardless of whether such protest takes place on the internet, in other virtual spaces or in physical spaces.

---

12 Big Brother Watch and others v United Kingdom, app nos. 58170/13, 62322/14 and 24960/15, 25 May 2021 [GC] ECHR, § 339.

13 n1, General Comment No. 37, at para. 10.

14 Overt surveillance encompasses any surveillance activities which the target(s) is made aware of. For example, where law enforcement have placed signs specifically stating that individuals are being subjected to surveillance within a specific area, or where individuals are made aware of surveillance through warnings that CCTV cameras are in operation.

15 Covert surveillance encompasses any surveillance activities conducted without prior notification to the target(s). This includes all surveillance activities conducted in a way or through means which intend to ensure that the target(s) are not made aware that they are being subjected to surveillance.

THE RIGHT TO PRIVACY: THE STARTING POINT FOR LEGAL LIMITS ON PROTEST SURVEILLANCE

What **standard of protection** should we be entitled to in relation to our rights to privacy and data protection when we are exercising our rights to protest and associate?

The human right to privacy protects our ability to remain anonymous and to control who has access to our personal, including sensitive, data at protests. It enables protesters around the world to participate safely in civic spaces, free from threats of discrimination, stigmatisation for their political beliefs, and persecution for objecting to the status quo. In this context, the UN Special Rapporteur on the rights of freedom of peaceful assembly and association's 2019 report to the UN Human Rights Council highlights the specific threats technology poses to freedom of assembly when it is used by states to "silence, surveil and harass dissidents, political opposition, human rights defenders [and] protesters."[16]

International human rights law protects the fundamental right to privacy[17] through two key principles: firstly, by establishing that every person has a right to respect for their private and family life, home, and correspondence. Secondly, by making any interference by a public authority with a person's right to privacy unlawful unless there is (a) a clear legal basis for the interference, and (b) the interference is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In order for an interreference to be deemed 'necessary' it must also be proportionate – any measure used to achieve any of the legitimate aims listed above should be the least invasive

16 UN Human Rights Council, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", (2019), UN Doc A/HRC/41/41, at para. 3, accessed online: https://undocs.org/A/HRC/41/41.

17 Universal Declaration of Human Rights (UDHR), Article 12, International Covenant on Civil and Political Rights (ICCPR), Article 17; Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"), Article 8; American Convention on Human Rights (ACHR), Article 11; Arab Charter on Human Rights (ArCHR), Article 17; Charter of Fundamental Rights of the European Union (CFR), Article 7.

option available to the relevant public authority.[18] Notably, Privacy International has published a detailed guide to International Law and Surveillance which collates the most relevant international law authorities on the right to privacy and surveillance.[19] In this paper, we rely mainly on jurisprudence interpreting and applying the right to privacy as enshrined by Article 8 of the European Convention on Human Rights (ECHR) as well as important observations, resolutions, and interpretive guidelines from UN bodies. Our aim is to use these legal authorities as a starting point to illustrate the human rights-based principles upon which a global movement to restrain protest surveillance can develop.

> Firstly, and as a starting point, **any processing of personal data in a protest context constitutes an interference with the right to privacy.**

It is well established in the jurisprudence of the ECtHR that "the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data."[20] The Court of Justice of the European Union (CJEU) has adopted a similar approach, establishing that "retention for the purpose of possible access is in itself an interference with [the rights to privacy and data protection]."[21]

---

18 See generally, UN Human Rights Council Resolution on the Right to Privacy In the Digital Age (2021), UN Doc A/HRC/RES/48/4, at recitals 2 and 6; See also, European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights", paras. 28-30, last updated on 31 August 2021, accessed online: https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

19 Privacy International, "PI's Guide to International Law and Surveillance", December 2021, accessible online: https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

20 S and Marper v the United Kingdom, app nos. 30562/04 and 30566/04, 4 December 2008 [GC] ECHR §121; See also, Leander v Sweden, app no. 9248/8126 March 1987, § 48.

21 Digital Rights Ireland Ltd v Ireland, C-293/12 and C-594-12, April 8, 2014, CJEU (Grand Chamber), § 29 .

Additionally, the UN High Commissioner for Human Rights[22] and the UN Human Rights Committee[23] have both made it clear that "the mere fact that a particular assembly takes places in public does not mean that participants' privacy cannot be violated. The right to privacy may be infringed, for example, by facial recognition technologies that can identify individual participants in a crowd. The same applies to the monitoring of social media to glean information about participation in peaceful assemblies."[24]

Therefore, the right to privacy applies to personal data that is generated in, or located in, the public space. Notably, when considering the impact of the collection and processing of personal data in public spaces, the ECtHR, has also found that "public information can fall within the scope of private life where it is systematically collected and stored in files held by authorities,"[25] especially where it can be shown that a person had a legitimate or reasonable expectation of privacy in relation to the information being collected, analysed, and retained.

We submit that by limiting the scope of the interference to systematic collection and storage, the position adopted by the ECtHR falls short of the robust safeguards that must be applied to surveillance of personal data that is generated at or located within protest contexts. Just as, "[t]he mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied….and thereby amounts in itself to an interference with the exercise […] rights under Article 8, irrespective of any measures actually taken against [someone],"[26] **we argue that the mere existence of the police power to overtly monitor, collect and retain protesters' personal data constitutes an interference with protesters' right to privacy**.

---

22 United Nations High Commissioner for Human Rights, "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests" (2020), at paras. 31-33, accessed online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement

23 The UN Treaty body that is responsible for monitoring the implementation of the International Covenant on Civil and Political Rights.

24 UN Human Rights Committee, General Comment No. 37 (129): On the right of peaceful assembly (article 21), (2020), UN Doc CCPR/C/GC/37, at paras. 61-62, accessed online: https://undocs.org/CCPR/C/GC/37.

25 Rotaru v Romania no. 2841/95, [GC] ECHR 2000, § 43.

26 Weber and Saravia v Germany, app. No 54934/00, 29 June 2006, §78; see also S and Marper v the United Kingdom, app nos. 30562/04 and 30566/04, 4 December 2008 [GC] ECHR.

Secondly, there must be an accessible, clear, comprehensive, and non-discriminatory legal basis for surveillance powers exercised by law enforcement at protests.

Additionally, the power to collect, analyse, use, and retain personal data about protesters through overt and covert surveillance before, during and after a protest must be subjected to transparent and robust safeguards to protect every person's right to privacy. This is also necessary to protect protesters' right not to have personal data collected indiscriminately simply due to the fact that they are exercising their basic freedoms.

In *M.M. v UK*[27], the ECtHR made it clear that, in relation to secret surveillance and covert-intelligence gathering, "it is essential…to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."[28] Importantly, the Court also held that:

> *[I]ndiscriminate and open-ended collection of criminal record data is unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, inter alia, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed.*[29]

Although the ECtHR has not applied its ruling from M.M v UK (which was specific to criminal record data) to personal, including sensitive, data collected in the context of protests,[30] **international human rights standards require personal data collected about protesters through overt and covert surveillance to be similarly**

27 M.M v the United Kingdom, app. No. 24029/07, 13 November 2012, ECHR.

28 n27, § 195.

29 n27, § 199.

30 Catt v the United Kingdom, app, no. 43514/15), 24 January 2019, ECHR § 102 – 104.

regulated.[31] The type of personal data that can be collected through emerging technologies deployed at protests must not be collected in an indiscriminate and open-ended way, and (as detailed in Sections IV and V below), must be subjected clears safeguards in order to protect the right to privacy and the rights to freedom of assembly.

> Finally, mere participation in a protest, in the absence of individualised suspicion, cannot justify the retention of personal data.

In *Catt v UK,*[32] the ECtHR held that the UK had violated Mr. Catt's rights under Article 8 of the ECHR. Mr. Catt was an active participant in a number of protest movements and regularly attended protests supporting trade unions, anti-war campaigns, and the UK's Labour Party. Even though he had never been convicted of any crime and had not been assessed to be a threat, the police in the UK refused to delete personal information about him contained in a national database.[33] The database identified Mr. Catt as having been present at or active in various protest movements. The police claimed that the retention of records relating to him would help "manage a future risk of crime".[34] The information held by the police was collected, analysed, and retained through "intelligence reports" which would have been the product of both covert and overt surveillance of protest movements by the police. In addition to complaining that "the systematic collection and retention of information about him in a searchable database amounted to an interference with his right to privacy under Article 8,"[35] Mr. Catt and a number of third-party interveners in this case submitted that **"the retention of such data was likely to have a chilling effect,"[36] especially "on legitimate political protests where [police databases] contain information about political activities.[37]**

---

31 Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/51/17, 4 August 2022, para. 56(d) and (e), accessible online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

32 n30.

33 This was a database used by the UK's "National Public Order Intelligence Unit".

34 n30, § 13.

35 n30, § 80.

36 ibid.

37 ibid, § 88.

The ECtHR found that, although there "was a pressing need to collect personal data" about Mr. Catt at protests, there was no pressing need to retain Mr. Catt's data. The Court emphasised that it reached this conclusion because:

> *[I]n the absence of any rules setting a definitive maximum time limit on the retention of such data the applicant was entirely reliant on the diligent application of the highly flexible safeguards in [the relevant guidance] to ensure the proportionate retention of his data. Where the state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive [...] Those safeguards must enable the deletion of any such data once its continued retention becomes disproportionate.*[38]
>
> *[...]*
>
> *Moreover, the absence of effective safeguards was of particular concern in the present case as personal data revealing political opinions attracts a heightened level of protection.* ***Engaging in peaceful protests has specific protection under Article 11 of the Convention*** *[freedom of assembly and association] which also contains special protection for trade unions, whose events the applicant attended.*[39]

38 ibid, § 119.

39 ibid, § 123.

The starting point is therefore that protest surveillance will be unlawful where:

- Law enforcement agencies are collecting, processing, and retaining personal, including sensitive, data about protestors without a clear and accessible legal basis for exercising these powers, and,
- Where such data is being processed and retained indiscriminately *without* safeguards which enable effective oversight of the lawfulness of the continued interference with protestors' privacy rights.

Notably, the UN Human Rights Committee's General Comment 37 highlights the relationship between the right to privacy and the right to freedom of assembly, arguably expanding on the basic starting position we outlined above. The UN Human Rights Committee pointed to the necessity of legal limits on protest surveillance based on the fundamental right to privacy: "Any information gathering…must strictly conform to applicable international standards, including on the right to privacy, and may never be aimed at intimidating or harassing participants or would-be participants in assemblies."[40]

Having broadly outlined how the right to privacy has been used to restrain protest surveillance, the following sections build on this starting point and argue for further safeguards. Section III explains why these safeguards are necessary to protect not only the right to privacy but, importantly, the right to freedom of assembly.

40 n1, General Comment No. 37, at paras. 61-62; See also, Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/51/17, 4 August 2022, accessible online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement.

III. THE RIGHT TO FREEDOM OF ASSEMBLY: STRENGTHENING THE LIMITS ON PROTEST SURVEILLANCE

The international and regional human rights law treaties that enshrine the right to freedom of assembly[41] as a fundamental right adopt a clear legal framework to assess the legality of interferences with the right to freedom of assembly: no restrictions shall be placed the right to freedom of peaceful assembly unless such restrictions are (a) prescribed by law; and (b) necessary in a democratic society in the interests of national security or public safety, public health or morals or the rights and freedoms of others. [42] Any restriction on the right to freedom assembly must not "be applied or invoked in a manner that would impair the essence of [the] right."[43] The right to freedom of assembly applies to everyone, and must be protected without discrimination on any ground, including race, nationality, sex, religion or immigration status.[44]

Importantly, in addition to the negative obligation on states to refrain from unjustified interferences with the right to freedom of assembly (often referred to as 'the obligation to respect'), international human rights standards impose a positive obligation on states to facilitate and protect the right to

41 Throughout this paper, we focus on the right to freedom of assembly as it encompasses the right to freedom of expression. The ECtHR addressed this overlap in the case of Ezlin v. France, no. 11800/85, 1991, at para. 35. The ECtHR held that Article 10 [freedom of expression] "is to be regarded as lex generalis in relation to Article 11 [the right to freedom of assembly and association], a lex specialis, so that it is unnecessary to take it into consideration separately." Cited in Ilia Siatitsa, "Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications", International Review of the Red Cross (2020), 102 (913), pp.181–198, at page 188.

42 International Covenant on Civil and Political Rights (ICCPR), Article 21; Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"), Article 11; African Charter on Human and Peoples' Rights (ACHP), Article 11; American Convention on Human Rights (ACHR), Article 15; Arab Charter on Human Rights (ArCHR), Article 24; Charter of Fundamental Rights of the European Union (CFR), Article 11.

43 UN Human Rights Committee, General Comment No. 31 (40): The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, (2004), UN Doc CCPR/C/21/Rev.1/Add. 13, at para. 6, accessed online: https://digitallibrary.un.org/record/533996?ln=en. See also, Galstyan v Armenia app. no. 26986/03, § 117, ECHR 2007.

44 ICCPR Article 2(1), ECHR Article 14.

freedom of assembly. As the ECtHR has noted, "States must not only refrain from applying unreasonable indirect restrictions upon the right to assemble peacefully but also safeguard that right."[45] In practice, this means that states have a legal obligation to anticipate and control counterdemonstrations when "peaceful demonstrations may annoy or give offence to persons opposed to the ideas or claims that it seeks to promote."[46] In this context, the ECtHR has held that "participants must…be able, with the State's assistance, to hold the demonstration without having to fear that they will be subjected to physical violence by their opponents."[47]

45 Kudrevičius and others v. Lithuania no. 37553/05, § 158, [GC] ECHR 2015. See also European Court of Human Rights, "Guide on Article 11 of the European Convention on Human Rights", para. 32-46, last updated on 31 December 2021, accessed online: https://www.echr.coe.int/Documents/Guide_Art_11_ENG.pdf.

46 Berkman v Russia no. 46712/15, § 47 ECHR 2021.

47 Plattform "Ärztefür das Leben" v. Austria, no. 10126/82, § 32, ECHR 1988.

HOW DOES PROTEST SURVEILLANCE INTERFERE WITH THE RIGHT TO FREEDOM OF ASSEMBLY?

The Special Rapporteur on the rights of freedom of peaceful assembly and of association has made clear recommendations to limit protest surveillance in order to protect freedom of assembly:

> *The use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited. Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision.*[48]

The Special Rapporteur has also highlighted how online spaces allow people from across the world to "participate in a virtually connected civil society"[49] and create a space for organising movements, such as the #MeToo movement and the #ClimateStrikes global movement. In the same report, the Special Rapporteur explicitly connected this with the importance of technologies which "enhance the security of civil society groups' digital communications."[50] This includes, for example "[e]ncryption technologies, pseudonymity, and other security features [which] have enabled individuals belonging to minority groups to find one another and create [communities].[51]

The relationship between the right to privacy and the right to freedom of assembly is therefore closely linked, and "a violation of the right to privacy, more often than not, is not an end in itself; it rather offers the means for infringing on

48 n16, at para. 57.

49 n16, at paras. 23-26.

50 ibid.

51 ibid.

other rights. In that sense, it often becomes the enabler for infringing on, among others, freedom of assembly."[52]

Surveillance of protesters and social movements must operate within a legal framework that balances social benefits of emerging technologies with their impact on our fundamental rights and freedoms. Restraints on protest surveillance must ensure that this form of policing is **subjected to the rule of law and the fundamental democratic principles of transparency and accountability.**

While we accept that the freedoms of assembly and association are qualified by the legitimate aims enshrined in international human rights law, including, for example, the need to prevent crime, protect others' rights, and protect public safety, **we oppose policing and surveillance practices which erode our freedom to organise and attend protests and ultimately, dissent**. In particular, mass surveillance of protests and social movements which is generalised, secretive, and not subjected to effective limitations and oversight mechanisms amounts to an unjustified interference with the right to freedom of assembly and a failure to secure the effective enjoyment of this right.

52 Ilia Siatitsa, "Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications", International Review of the Red Cross (2020), 102 (913), pp.181-198, at page 190.

The hidden sanctions of unlawful protest surveillance

- Firstly, unlawful and mass surveillance indiscriminately subjects protesters to hidden sanctions including, for example, profiling, being virtually stopped-and-searched without limitation, discrimination, and breaches of the right to privacy.
- Secondly, it can be used to facilitate persecution and criminalisation of dissent.
- Third, it deters people from using civic spaces to exercise their fundamental rights.[53]

(Section V of this paper provides detailed examples and analysis of how certain types of protest surveillance can subject protesters to these hidden sanctions).

The omnipresence of highly intrusive surveillance technologies at protests necessarily means that anyone who considers organising or attending a protest must either knowingly or unknowingly subject their personal data – including for example, their private messages and photographs, their political opinions, or even their sexual orientation – to unregulated collection and analysis by law enforcement. **At the core of our argument against mass surveillance is the position in international human rights law that restrictions on freedom of assembly "need to be specific and necessary to achieve a specific legitimate aim;** [and that] there needs to be a rational connection between the measure and the prescribed aim, meaning that **a measure cannot be based on an abstract aspiration that it might facilitate the aim."**[54] In a democratic society,

53 For PI's full analysis on the impact of surveillance on civic spaces, democracy and dissent, see Privacy International, "Protecting civic spaces: defending democracy and dissent", May 2019. See also, Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/51/17, 4 August 2022, para. 47, accessible online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

54 Aharon Barak, "Rational Connection", in Proportionality: Constitutional Rights and their Limitations, Cambridge University Press, Cambridge, 2012, pp. 303–316, cited in Ilia Siatitsa (n53) at page 191.

people should not have to choose between their right to privacy and their rights to freedom of assembly and expression.

In the following section, we summarise the legal limits which are necessary for protest surveillance to be lawful and compatible with international human rights standards. In Section V, we sketch the 'timeline' of a protest to expand on these standards by illustrating the circumstances in which protest surveillance is being deployed and how it interferes with the rights to privacy and the right to freedom of assembly at every 'stage' of a protest.

IV. HUMAN RIGHTS STANDARDS FOR RESTRAINING PROTEST SURVEILLANCE

1. Any information gathering activities which have the effect of collecting, processing, and retaining any amount of personal data about protesters – whether publicly available or not, and whether obtained by overt or covert means, must be considered an interference with the right to privacy and a form of surveillance, and must fall within a statutory framework which places limits on surveillance and data collection powers.

2. Any processing, including collection, analysis, use and retention of personal data before, during and after a protest constitutes an interference with the right to privacy. People's right to privacy must be protected while they associate, participate in organising assemblies, and while attending assemblies even where such assembles are considered public or where protesters have shared information in a way which may be considered public.

3. Indiscriminate, generalised, and mass protest surveillance is unlawful.

4. Any power to undertake overt and targeted protest surveillance may only be lawful where:

    a. it adheres to requirements under international human rights law (is based on a clear, accessible, and transparent legal basis; it is targeted at a specific individual, is necessary in a democratic society to achieve the legitimate aims outlined within the rights to privacy and freedom of assembly; is the least intrusive means by which that legitimate aim can be achieved, both in the context of the right to privacy and freedom of assembly (i.e. the impact of

the targeted surveillance on the right to privacy and freedom of assembly is proportionate to the legitimate aim being pursued); and there are appropriate and robust safeguards in place).

5. Any power to undertake covert and targeted surveillance may only be lawful where:

   a. it adheres to requirements under international human rights law (as outlined above at 4a);

   b. there is prior, explicit authorisation to process a targeted individual's personal data on the basis of reasonable suspicion that it is necessary to prevent a serious criminal offence.

6. Any power to undertake protest surveillance must be subjected to transparent and robust safeguards and limitations. This includes information security safeguards (including encryption of audio-visual footage collected at protests), access limitation and warrant-based access, limits on retention, effective oversight mechanisms, and effective and accessible mechanisms for protesters and organisations to challenge any form of surveillance they are exposed to.

7. Biometric data-collecting technologies should never be deployed during protests. Any power to collect sensitive, including biometric, data may be lawful only where (a) it is targeted and (b) there is prior, authorisation to obtain, process, and retain such targeted individual's biometric data and (c) such prior authorisation is based on a reasonable suspicion that this is necessary to prevent a serious criminal offence.

8. In the absence of individualised reasonable suspicion, it is unlawful to retain protesters' personal data merely because they participated in a protest. Any personal data collected incidentally must be deleted without undue delay.

9. Before any surveillance technologies are acquired by police and/or other law enforcement agencies, they must be subjected to human rights impact assessments, including, in particular impact assessments on the rights to privacy and freedom of assembly, as well as equality impact assessments and data protection impact assessments.

10. It is unlawful to undertake any form of protest surveillance on the basis of race, ethnicity, sex, religion, political or other opinion, national or social origin, association with a national minority, property, birth, or other status.[55]

11. Predictive policing technologies intended to gather generalised data should never be deployed during protests. Additionally, predictive policing cannot be used as a blanket justification by police and/or law enforcement to collect and retain personal data about protesters without limitation.

12. Whenever a relevant authority exercises a power to undertake targeted protest surveillance, such authority must be under an obligation to inform and/or notify each individual that their personal data has been collected as a result of targeted protest surveillance without undue delay following the end of any criminal investigation. Any notification must be accompanied by an effective and exercisable right for individuals and/or organisations to challenge the lawfulness of protest surveillance and to seek remedies for unlawful protest surveillance.

55 For further research around ethnic minorities being placed at risk of heightened surveillance and therefore interferences with their fundamental human rights, see, Privacy International, "Ethnic minorities at greater risk of oversurveillance after protests", 15 June 2020, accessible online: https://bit.ly/3d42tJx.

V. THE TIMELINE OF A PROTEST: MAPPING INTERFERENCES AND SAFEGUARDS AT EVERY STAGE OF A PROTEST

In this section, we attempt to sketch the various ways in which individuals 'participate' in collective association, assembly, and protest. Our aim is to illustrate that the right to freedom of assembly applies before, during, and after a protest or assembly takes place. As a result, protest surveillance which is conducted against individuals at any of these 'stages' **may violate fundamental human rights and impede our ability to dissent and express ourselves collectively.**

The UN Human Rights Committee has made it clear that:

> *Article 21 and its related rights do not only protect participants while and where an assembly is ongoing. Associated activities conducted by an individual or by a group, outside the immediate context of the* ***gathering but which are integral to making the exercise meaningful are also covered.*** *The obligations of State parties thus extend to actions such as participants' or organisers mobilisation of resources; planning; dissemination of information about an upcoming event…communication between participants leading up to and during the assembly, broadcasting of or from the assembly; and leaving the assembly afterwards. These activities may, like participation in the assembly itself, be subject to restrictions, but these must be narrowly drawn.* ***Moreover, no one should be harassed or face other reprisals as a result of their presence at or affiliation with a peaceful assembly.***[56]

56 n1, General Comment No. 37, at para. 33.

BEFORE A PROTEST: ORGANISING, PLANNING, ASSOCIATING

The right to freedom of assembly under international human rights law protects the process of organising a protest and the right to associate and meet in the course of preparing for protest:[57] States have an obligation to respect and ensure peaceful assemblies "before, during and after assemblies".[58] Both the ECtHR and the CJEU have recognised that the right to freedom of association, "does not only include the ability to create or dissolve an association but also covers the possibility for that association to act in the meantime, which means…that it must be able to pursue its activities and operate without unjustified interference by the State."[59]

It is important to situate the right to organise and associate within the context of 'how we protest' today. Of course, 'organising' or 'associating' can happen in person, but it also increasingly takes place online – through social media platforms, group chats on instant messaging applications, and video-conferencing software. In this context, and before a protest even takes place, law enforcement and security agencies have the capacity to deploy a wide range of surveillance technologies to gather information about protestors. They collect and analyse information about the date and time of protests, but they may also collect personal, including sensitive, data about anyone who is using the internet to plan protest actions, associate with political groups, express a political belief collectively or to agitate for social change. As the UN Commissioner for Human Rights has recently highlighted, "modern data-driven technologies are dramatically shifting the balance of power between the entity carrying out the surveillance and those being monitored. Before the advent of large-scale automated surveillance and data analytics tools, there were practical limitations to surveillance that provided a certain level of protection for individuals… Sophisticated digital tools render those past "natural" protections moot."[60]

57 ibid at para. 12 (emphasis added).

58 n1, General Comment No. 37, at para. 23.

59 European Commission and Kingdom of Sweden v Hungary, C-78/18, Para 110, CJEU 2020; See also Moscow Branch of the Salvation Army v Russia, no. 72881/01, ECHR §

60 n31 at para. 38.

Examples of surveillance deployed before a protest

"Social Media Intelligence Gathering" ("SOCMINT") refers to the techniques and technologies that allow companies and/or governments to monitor social media networking sites (SNSs), such as Facebook or Twitter.[61] PI has released guides explaining how law enforcement in the UK may use SOCMINT in protests contexts.[62] Broadly, law enforcement agencies may undertake SOCMINT in the following ways:

- **Open-source SOCMINT monitoring:** this includes using a specific software and 'feeding it' (or inputting) a string of keywords to produce "an overview of the instances of online communication and their locations (forums, Facebook pages, Twitter accounts, etc.) in which these keywords are used,"[63] and monitoring a specific set of discussion forums, individuals, and groups within SNSs. This is often referred to as 'open-source' intelligence gathering as agents will focus on gathering information that is ostensibly publicly available without using techniques such as hacking. Nevertheless, it is often conducted covertly – that is, without ever notifying the target that they are being subjected to surveillance.
- **Non-open source SOCMINT monitoring:** law enforcement may deploy intelligence gathering techniques which allows them to access to personal data that is not restricted to what is traditionally considered 'open-source'. For example, by using fake profiles to access closed groups and private profiles. This may also include instances where police forces deploy basic 'trackers' (similar to the ones advertisers use) to follow people's internet

61 Privacy International, "Social Media Intelligence", 23 October 2017, accessed online: https://privacyinternational.org/explainer/55/social-media-intelligence

62 Privacy International, "Free to Protest Guides (UK Edition): How Social Media Monitoring can be used at a protest and how you can minimize risks to your data", last updated June 2021, accessed online: https://privacyinternational.org/sites/default/files/2021-06/socmint.pdf.

63 Victor Bekkers et.al, "Social media monitoring: Responsive governance in the shadow of surveillance?", (2013), Government Information Quarterly (30): 335-342, at p. 4.

- activity. Additionally, police agents undertaking these activities may be using technology which enables them to access information or communications which individuals reasonably expect to be private. For example, instant messages on various messaging platforms, including 'closed' group messages or person-to-person messages, especially where services are unencrypted.
- **"Scraping" websites and creating databases:** law enforcement may use software to indiscriminately 'scrape' all available data that is relevant to a specific topic or search term from various SNS sources. This data could then be disaggregated, analysed, and stored in law enforcement databases for indefinite periods.
- **Analysis and prediction:** Using personal data that is collected through SOCMINT and scraping methodologies, law enforcement agencies may build profiles on protestors and protest movements and to generate 'predictive' conclusions about individuals and/or groups.

In 2020, the Intercept reported that a company called DataMinr shared data about Black Lives Matter protests and protestors with police forces across the US, allowing law enforcement to digitally monitor the movement and, "tipping off police to social media posts with the latest whereabouts and actions of demonstrators." This included the location of planned protests before they took place and images of Black Lives Matter protesters.[64] DataMinr is one of a number of companies which has heightened access to Twitter data (through "a specific stream of data called 'firehose' data that allows DataMinr to scan every public tweet as soon as it is sent out" via an agreement with Twitter). Separately, in the UK, the independent inspectorate for police and fire forces ("HMICFRS")

64 Sam Biddle, "Police Surveilled George Floyd Protests With Help From Twitter-Affiliated Startup Dataminr", The Intercept, 9 July 2020, accessed online: https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/. See also, Matt Cagle, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color", American Civil Liberties Union, 11 October 2016, accessed online: https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target

has proposed creating an offence of "using social media platforms to cause intentional mass disruption."[65] This illustrates how police forces around the world are increasingly expanding their ability to deploy SOCMINT to monitor and surveil protest movements.

In some instances, police are allegedly deploying additional interception techniques such as hacking in order to engage in "cyber-patrolling" to indiscriminately monitor activists, political groups, and protest organisers in the lead up to protests. In 2021, Colombia witnessed an unprecedented, countrywide uprising, with thousands of people protesting against "deep inequality in the distribution of wealth; poverty […] and access to economic, social, and cultural rights, [as well as] high levels of violence and impunity, [and] ethnic-racial and gender discrimination."[66] The protests were met with severe brutality by police and specifically, the Mobile Antiriot Squad of the National Police – a police unit which Colombia's Supreme Court of Justice has described as posing "a serious and present threat to those seeking to go out and demonstrate to peacefully express their opinions, as its actions, far from being isolated are consistent and reflect ongoing and identifiable aggression during protests."[67] At the same time, throughout the uprising, human rights groups documented complex and opaque instances of cyber-patrolling by the cybercrime units of Colombia's police, armed forces, and intelligence agencies. **Human rights organisations highlighted that those agencies refused to provide any information around what kind of personal information was being collected about protesters and importantly, the basis on**

65 HMICFRS, "Getting the balance right? An inspection of how effectively the police deal with protests", 6 May 2021, Proposal 17, accessed online: https://www.justiceinspectorates.gov.uk/hmicfrs/publication-html/getting-the-balance-right-an-inspection-of-how-effectively-the-police-deal-with-protests/#2-police-intelligence-about-protests.

66 Inter-American Commission on Human Rights, "Observations and recommendations: working visit to Colombia", June 2021, at para. 2, accessed online: http://www.oas.org/en/iachr/reports/pdfs/ObservacionesVisita_CIDH_Colombia_ENG.pdf

67 Colombia Supreme Court of Justice, Civil Cassation Chamber, STC 7641-2020 (September 22 2020), cited in Inter-American Commission on Human Rights, "Observations and recommendations: working visit to Colombia", June 2021, at paras. 19-21, accessed online: http://www.oas.org/en/iachr/reports/pdfs/ObservacionesVisita_CIDH_Colombia_ENG.pdf

which certain activities were being investigated for "digital terrorism" – which included accusations such as "lying about actions by [security forces]".[68]

Without effective legal constraints on the extent of surveillance police and law enforcement can undertake before a protest, anyone who even considers exercising their right to organise a protest or associate online could face disproportionate intrusions into their private lives, have sensitive information about their political beliefs collected and stored indefinitely, be subjected to profiling based on an opaque aggregation of data points available online (including socio-economic background, ethnicity, nationality, and political or religious beliefs), and, crucially, may even be criminalised as a result of this type of profiling. Often, protestors do not even know that they are being subjected to these types of sanctions because of the lack of legal frameworks requiring notification, transparency, and accountability. The only way for individuals to avoid these 'hidden' sanctions will be to refrain from exercising their rights to organise and assemble online.

68 Fundación Para La Libertad de Prensa, "Los jueces de la verdad, el mar de mentiras detrás del ciberpatrullaje del Estado", 29 October 2021, accessed online: https://flip.org.co/index.php/es/informacion/pronunciamientos/item/2817-los-jueces-de-la-verdad-el-mar-de-mentiras-detras-del-ciberpatrullaje-del-estado; See also: Fundación Karisma, "Organizaciones advierten riesgos de tecnologías de vigilancia en audiencia ante la CIDH", 29 October 2021, accessed online: https://web.karisma.org.co/organizaciones-advierten-riesgos-de-tecnologias-de-vigilancia-en-audiencia-ante-la-cidh/

Applying the legal standards

What limits should be placed on law enforcement's ability to capture, use, and store personal, identifying, and sensitive data about civilians who organise protests **before a protest has even taken place?**

We recognise that in order to uphold states' positive obligation to protect the right to freedom of assembly, international human rights standards emphasise that law enforcement should be in communication with organisers. This allows law enforcement to obtain information to facilitate appropriate protections for protesters, especially from counterdemonstrations.[69] This is known as the duty to take "reasonable and appropriate measures to enable lawful protests to proceed peacefully."[70] In this regard, the ECtHR has found that prior authorisation procedures – that is, administrative rules requiring public assemblies to be subject to 'authorisation' are lawful **"as long as the purpose of the procedure is to allow the authorities to take reasonable and appropriate measures in order to guarantee the smooth conduct of any assembly."**[71]

We submit that information gathering tactics deployed by law enforcement before a protest takes place must be similarly restrained.

> Firstly, and in accordance with the standards outlined above, this type of surveillance must not be indiscriminate and it must adhere to fundamental human rights standards. Therefore, it must be targeted at specific individuals and the (i) type and (ii) amount of personal data collected and processed through information gathering techniques deployed before a protest must not exceed what is strictly necessary to facilitate an assembly.

For example, if a police force has a legal basis for deploying SOCMINT, they must be limited to gathering information related to the timing of a protest, routes, and key contacts to communicate with. It may also be appropriate for data which contains personally identifying information to be anonymised and/or

69 See for example, UN Human Rights Council, "Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies", (2016), UN Doc A/HRC/31/66, at paras. 37-49, accessed online: https://undocs.org/A/HRC/31/66; See also, Frumkin v Russia, no. 74568/12, § 128-130, ECHR (2016).

70 European Court of Human Rights, "Guide on Article 11 of the European Convention on Human Rights", pp. 32-46, last updated on 31 December 2021, accessed online: https://www.echr.coe.int/Documents/Guide_Art_11_ENG.pdf.

71 Sergey Kuznetsov v. Russia, app no. 10877/04, 23 October 2008. ECHR, § 42.

depersonalised in the first instance. It would not be proportionate, for example, for law enforcement to collect and process information about organisers permanent home address, nationality, or past protest activities. Additionally, it is not proportionate to deploy "scraping" software to collect mass personal data about protesters.[72]

> Secondly, law enforcement should not deploy covert surveillance (whether generalised or targeted) to obtain information related to the organising of a protest unless there are reasonable grounds to suspect that a particular individual or group will commit a serious crime in the context of a specific protest.

Covert surveillance constitutes an interference with the right to privacy and it would be disproportionate to seek to obtain information that would facilitate an assembly through covert surveillance when that information may be obtained through less intrusive means.

> Third, in circumstances where protest surveillance before a protest is not undertaken on the basis of reasonable suspicion of criminal activity, law enforcement should be legally required to notify individuals that they are being subjected to surveillance. This would ensure that protest surveillance which takes place before a protest is generally overt. Additionally, law enforcement should be under an obligation to make publicly available the methodologies and practices they are lawfully permitted to deploy to gather information before a protest takes place.

> Finally, personal data collected by police for the purposes of facilitating a protest must not be retained after the protest has taken place unless such data is relevant to ongoing criminal investigations.

As outlined in the safeguards, police forces should not rely on blanket justifications that such data may be useful for predictive policing in the future.

72 n31, para.51.

DURING A PROTEST: ATTENDING A PROTEST

The right to freedom of assembly under international human rights law protects a broad range of protest actions, from one-person-protests and mass marches to spontaneous roadblocks, online protests and other forms of disruptive action intended to draw attention to a wide variety of social issues. While states have the power (and obligation) to maintain public order and ensure that protesters and the public are protected during a protest, **police powers which place restrictions on core aspects of freedom of assembly to achieve these legitimate aims amount to an interference with the right to freedom of assembly.** Therefore, in order to be lawful, any such interferences or restrictions must have a basis law, be compatible with the rule of law and afford adequate legal protection against arbitrariness.[73] Additionally, they must be a necessary and proportionate means of maintaining public order and preventing serious crime during protests.

We argue that the power to surveil protesters must be understood as one type of police power – similar to, and alongside, other police powers such as the power to make arrests, or the power to stop-and-search individuals on the basis of reasonable suspicion. While we accept that the use of these police powers at protests may be necessary and proportionate in certain, prescribed, circumstances, effective limits and restraints are necessary to prevent abuse and respect the right to freedom of assembly. As has been highlighted by various experts on the right to freedom of assembly, **surveillance deployed at protests "creates a climate of fear and has a chilling effect on the right to freedom of peaceful assembly."[74]** Further, surveillance technologies have the potential to "identify and threaten, attack, criminalize or otherwise [...] deter peaceful assembly organizers and participants."[75] In order to be lawful, protest surveillance must only be exercised in way which helps police manage protests, not shut them down all together by interfering with core aspects of the right.

---

73 Lashmankin and Others v. Russia, apps. No 57818/09, 51169/10, 4618/11 et. al., 7 February 2017, ECHR §§ 410-4713; See also, M.M. v the United Kingdom cited at n27 § 193.

74 OHCHR, Joint Declaration on Protecting the right to freedom of assembly in times of emergencies", 15 September 2022, accessible online: https://www.ohchr.org/sites/default/files/documents/issues/fassociation/2022-09-15/JointDeclarationProtectingRightFreedominTimesEmergencies15Sept2022.pdf

75 ibid.

Two core aspects of the 'essence' of freedom of assembly are, firstly, the ability to participate in a protest without retribution,[76] and secondly, the presumption that assemblies are peaceful.[77]

When deciding whether or not to participate in a protest, people around the world often "rely on the anonymity of the crowd to protect themselves against retribution, particularly in contexts where any form of dissent is suppressed."[78] This allows people and groups to freely express their views without fear of being identified and targeted for reprisal. As we have already highlighted, every person has the right to freedom of assembly, and it is unlawful for states to impose restrictions which are either directly or indirectly discriminatory on the basis of race, sex, religion, political opinion, or nationality. For example, a person with temporary or irregular migration status should have the right to protest anonymously, without fear that their attendance at a protest will be recorded and shared with law enforcement or other agencies making decisions about their right to remain in a given country. Additionally, if an individual wants to attend a protest in support of LGBT+ rights but does not want a 'record' of their presence at a protest for personal reasons, they have a reasonable expectation that the privacy of their identity (that is, their anonymity) will be maintained. Similarly, if someone wants to attend a protest in support of a controversial belief, such as an anti-vaccination or anti-lockdown protest, but they do not want a record of this information, they will also have a reasonable expectation that the privacy of their identity would be maintained.

Further, **the legal presumption in favour of treating assemblies as peaceful is fundamental to the right to freedom of assembly because it acts as a check on states which seek to criminalise protest actions or dissent merely on the basis of the potential for violence.** The ECtHR has held that:

> *[A]n individual does not cease to enjoy the right to freedom of peaceful assembly as a result of sporadic violence or other punishable acts*

76 n52, at page 194.

77 Venice Commission and OSCE/ODIHR "Guidelines on Freedom of Assembly", (2019), CDL-AD(2019)017, para. 30, accessed online: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2019)017rev-e.

78 n52, at page 194.

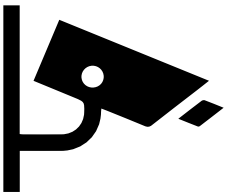
> *committed by others in the course of the demonstration if the individual in question remains peaceful in his or her own intentions or behaviour […] Even if there is a real risk that a public demonstration might result in disorder as a result of developments outside the control of those organising it, such a demonstration does not as such fall outside the scope of [the protections afforded by the right to freedom of assembly], and any restriction placed thereon must be in conformity with the terms of [the relevant Convention] provision.*[79]

This position is in line with the UN Human Rights Committee's interpretation of the right to freedom of assembly, which makes it clear that "any restrictions on participation in peaceful assemblies should be based on a differentiated or individualised assessment of the conduct of the participants and the assembly concerned. Blanket restrictions on peaceful assemblies are presumptively disproportionate."[80]

79 n46, at § 94.

80 n1, General Comment No 37, at para. 38

Examples of surveillance deployed during a protest



We can categorise the most prevalent surveillance technologies deployed at protests into groups based on the methodologies they rely on to collect and analyse data about protesters:

METHODOLOGY	EXAMPLES OF TECHNOLOGY
Monitoring, tracking and raw image collection	IMSI catchers, CCTV cameras, bodycams, SOCMINT, drones, and biometric surveillance technologies (e.g., facial recognition technology and gait recognition software).
Interception and extraction	Examples include hacking/malware, mobile phone extraction tools, cloud-data extraction tools.

- **IMSI catchers (or "Stingrays")** are surveillance devices which can be used by police forces at protests to capture information about the mobile phones. When used at protests, IMSI catchers record the presence of mobile phones[81] by deploying a "fake" mobile

81 Privacy International, "How IMSI catchers can be used at a protest", 5 May 2021, accessible online: https://privacyinternational.org/explainer/4492/how-imsi-catchers-can-be-used-protest. See also, Privacy International "Information Tribunal Decisions re IMSI Catchers: A loss for transparency and why we will continue to fight through other means", 12 June 2020, accessible online: https://privacyinternational.org/long-read/3925/information-tribunal-decisions-re-imsi-catchers-loss-transparency-and-why-we-will

phone mast within its vicinity whose only job is log the globally unique 'mobile subscriber identity' of the phones it tricks into connecting to it (some models will also intercept calls and text messages).[82]

- **CCTV, cameras attached to drones, and police bodycams** create audio-visual records which can be then used to document a person's identity, who they are associating with and what their beliefs are.
- **Biometric surveillance technologies:** facial recognition-enabled cameras (and gait-recognition enabled cameras) can capture footage and identify people in real-time or at a later point.[83] Crucially, this type of surveillance collects biometric data– a type of personal data which highly sensitive and therefore should be subjected to stringent safeguards.[84]
- **Malware which enables hacking, cloud extraction technology** and **mobile phone extraction tools (MPE)**, all have the same effect: covertly intercepting private communications and obtaining personal data, including sensitive, data over which protesters have a clear expectation of privacy.

In 2022 it was reported that the Israeli security forces used "mobile-phone tracking technology to monitor and threaten Palestinian protesters"[85] who were classified as having been in the "area" where protests and clashes with riot police took place. The 'area' was Al Aqsa Mosque in Jerusalem during Ramadan.

82 Privacy International, "IMSI catchers: PI's legal analysis", 25 June 2020, accessible online: https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis; See also, Privacy International, "IMSI catchers: facilitating indiscriminate surveillance of protesters", 19 June 2020, accessible online: https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters.

83 Privacy International, "How facial recognition technology can be used at a protest", 5 May 2021, accessible online: https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest

84 Privacy International, "IMSI catchers: PI's legal analysis", 25 June 2020, accessible online: https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis; See also, Privacy International, "IMSI catchers: facilitating indiscriminate surveillance of protesters", 19 June 2020, accessible online: https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters.

85 Josef Federman, "Israel upholds use of surveillance technology on protesters", 2 February 2022, Associated Press and ABC News, accessed online: https://abcnews.go.com/International/wireStory/israel-upholds-surveillance-technology-protesters-82628174.

Israel's domestic intelligence agency "sent a text message to people […] and told them '[W]e will hold you accountable' for acts of violence."[86] This was sent to hundreds of people who happened to be around a religious site, many of whom were not even at the protests but had attended prayers at the mosque or live and work nearby. Following a legal challenge by a human rights group around the law enforcement's use of this technology, Israeli authorities acknowledged that the mass distribution of the text messages included unintended targets but refused to discontinue its use. In a context where international human rights organisations have documented "discriminatory arrests"[87] by Israeli police targeting Palestinians as well as "torture" and "unlawful force", the use of technology which monitors, tracks, and identifies protestors on a mass scale constitutes a clear threat to people's safety, as well as the threat of criminalisation when exercising their right to nonviolent protest.

These technologies represent a sample of the ever-growing array of surveillance tools that law enforcement agencies deploy during protests. These tools can be deployed covertly and indiscriminately, they have the ability to collect highly intrusive personal, including sensitive data. They enable law enforcement to monitor, track, and document every individual protester's location, identity, speech, and the 'group' or association with whom they attend the protest. This can then even be linked to data gathered before a protest or other existing data within various agencies' databases.

We have previously argued that deploying these surveillance technologies at protests without any restrictions turns protests into a modern 'panopticon', whereby protesters are aware that they might be being watched, leading them to modify their behaviour accordingly and therefore act as if they are being watched, **perhaps [people] might think twice about even attending a protest because [they] don't want to trade [their] right to protest with [their] right to privacy.**[88]

86 ibid.

87 Amensty International, "Israeli police target Palestinians with discriminatory arrests, torture and unlawful force", 24 June 2021, accessed online: https://www.amnesty.org/en/latest/news/2021/06/israeli-police-targeted-palestinians-with-discriminatory-arrests-torture-and-unlawful-force/

88 Privacy International, "Can we be free to protest in an age of high tech police surveillance of protests?" 29 June 2021, accessed online: https://privacyinternational.org/news-analysis/4581/can-we-be-free-protest-age-high-tech-police-surveillance-protests

Generalised information gathering at protests, indiscriminate surveillance, and targeted covert surveillance that is not based on reasonable suspicion, all interfere with core aspects of the right to freedom of assembly. Without restraints on protest surveillance, it is impossible for groups or individuals to protect their anonymity and their privacy at protests. Further, by interfering with every protester's right to privacy on the basis that it is necessary to protect public order and the prevent crime, unrestrained protest surveillance treats every protester as 'suspect', and therefore, undermines the legal presumption in favour of treating assembles as peaceful. Finally, unrestrained protest surveillance has substantial chilling effect on freedom of assembly. In the absence of limitations on police powers to surveil individuals and groups during assemblies, protest surveillance amounts to an **unlawful restriction on the essence of freedom of assembly.**

Applying the legal standards

The ability to protect your communications, personal data, identity, and audio-visual footage of you at a protest from being recorded and maintained by the police is fundamental to enabling free participation and expression on major social issues.

> **Firstly, protest surveillance which indiscriminately monitors, tracks, and collects footage of protestors forces individuals to choose between protecting their anonymity and exercising their right to protest. This undermines a core aspect of the right to freedom of assembly and therefore, should be unlawful.**

Additionally, biometric surveillance of protesters should never be used to identify those peacefully participating in a protest. PI supports the UN High Commissioner for Human Rights' recommendation that states should impose moratoriums on the use of high-risk technologies such as "remote real-time facial recognition" in public spaces at least until it is ensured that they can be used without violating human rights."[89] The Commissioner has highlighted that,

> *Recording, analysing, and retaining someone's facial images without her or his consent constitute interferences with a person's right to privacy. By deploying facial recognition technology at assemblies, these interferences occur on a mass and indiscriminate scale, as this requires the collection and processing of facial images of all persons captured by the camera equipped with or connected to a facial recognition technology system.*[90]

Unless the relevant authorities are able to show that they have concrete and reasonable suspicion that either (i) specific participants are engaging in a serious criminal offence or (ii) an individual who is being investigated for a criminal offence is likely to be present, the use of biometric surveillance is unlikely

89 UN Human Rights Council, "The right to privacy in the digital age: report of the High Commissioner for Human Rights , (2021), UN Doc A/HRC/48/31, para. 59 (d), accessed online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement

90 UN Human Rights Council, "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests", (2020), UN Doc A/HRC/44/24, para. 33, accessed online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement

to be a proportionate means by which to achieve general policing ends. This is particularly so because even if a protest turns violent, facial recognition technology deployed at a protest is unlikely to be a necessary or effective means of managing the protest. This means it will not be the most effective and least intrusive means of achieving the legitimate aim of protecting public order.

Second, and as regards mass interception techniques, the ECtHR has already found that indiscriminate interception or, generalised recording of communications by law enforcement authorities can amount to an interference with the right to freedom of expression.[91] In this context, the Court has maintained a distinction between whether or not the 'generalised recording of communications' targets journalists or journalistic sources[92] and where there are safeguards for journalistic material.[93] A key part of the ECtHR's ruling in the case of Big Brother Watch and others was that without adequate safeguards in place to protect journalistic material, bulk interception of communications data and communications content will likely violate the right to freedom of expression.[94]

> We can apply this reasoning to the right to freedom of assembly: when law enforcement agencies are empowered to deploy technologies which indiscriminately intercept and extract communications and personal data during protests, without any safeguards or limitations on these police powers, **this amounts to an unlawful interference with protestors' rights to both freedom of assembly and expression.**

Third, we argue that some of the technologies that law enforcement can deploy when undertaking targeted surveillance that is covert effectively subject protestors to constant, virtual and hidden stop-and-searches. This type of surveillance often takes place at protests even without justifiable grounds or

91 n26 (Weber).

92 ibid, §151.

93 Big Brother Watch and others v United Kingdom, app nos. 58170/13, 62322/14 and 24960/15, 25 May 2021 [GC] ECHR, § 456 – 458.

94 ibid.

reasonable suspicion. Instead of being physically stopped-and-searched, protesters are being searched in real time through technologies which enable invasive access to personal, including sensitive, information that they carry around on their devices.

> Much like police powers to physically stop-and-search individuals,[95] police powers to 'virtually' and covertly search protesters **must be authorised only on the basis of reasonable suspicion** that it is necessary to prevent a serious criminal offence.

For example, authorities must have credible evidence that, before or during a protest, "certain participants are inciting others to use violence, and such actions are likely to cause violence; that the participants have violent intentions and plan to act on them; or that violence on their part is imminent."[96] That has to be determined on a case-by-case basis – for example, if police have intelligence which says that protesters are carrying objects that could be protective equipment such as gas masks or helmets is not necessarily sufficient to deem those participants' conduct violent and therefore subject them to targeted surveillance.

Without these safeguards, the use of these surveillance powers is left open to abuse – particularly in order to silence dissent.

95 See n1, General Comment No. 37 para. 83: "Powers of "stop and search" or "stop and frisk", applied to those who participate in assemblies, or are about to do so, must be exercised based on reasonable suspicion of the commission or threat of a serious offence, and must not be used in a discriminatory manner. The mere fact that authorities associate an individual with a peaceful assembly does not constitute reasonable grounds for stopping and searching them."

96 n1, General Comment No. 37, para. 19.

AFTER A PROTEST: WHAT HAPPENS TO PROTESTERS' DATA AFTER THEY HAVE PARTICIPATED IN PROTEST?

Under international human rights law, the positive obligation on states to uphold the right to freedom of assembly means that states must refrain from pursuing policies or practices which can reasonably be said to deter people from exercising their right to protest. Creating and maintaining police databases which retain unlimited amounts of personal data about protesters, and then using these databases for 'predictive policing', especially in order to monitor protestors, amounts to unlawful protest surveillance and will inevitably have a chilling effect on the enjoyment of the right to protest.[97]

In the case of Ezlin v France,[98] the ECtHR dealt with a question of whether a "non-punitive sanction" imposed in relation to an individual's involvement in a demonstration could constitute a violation of the right to freedom of assembly. The Court found that the term 'restrictions' in the text of Article 11 ("no restrictions shall be placed on the exercise of [the right to freedom of peaceful assembly and to freedom of association with others"]), includes measures taken after a protest.[99] In this context, a lawyer who had taken part in a protest during which criminal damage had occurred, but crucially, during which no criminality on the part of the lawyer was proven or even charged, could not be subjected to disciplinary proceedings by the relevant Bar Council merely for failing to "dissociate" himself from other demonstrators' offensive or insulting acts.[100] This was found to be an unjustified restriction on the right to freedom of assembly.

97 n31, para.47.

98 Ezlin v France, app. no. 11800/85, 26 April 1991, ECHR.

99 ibid., § 39.

100 ibid., § 41.

More broadly, the ECHR has consistently ruled that interferences with the exercise of the freedom of peaceful assembly can take various forms, ruling that to amount to an interference, government action:

> *[D]oes not need to amount to an outright ban, legal or de facto, but can consist in various other measures taken by the authorities. The term 'restrictions'…must be interpreted as including both measures taken before or during an assembly, and those, such as punitive measures taken afterwards. For instance, a prior ban can have a chilling effect on the person who intend to participate in a rally and thus amounts to an interference, even if the rally subsequently proceeds without hindrance on the part of the authorities.*[101]

101 Kasparov and others v. Russia, no. 21613/07, § 84, ECHR 2013; See also Bączkowski and Others v. Poland, no. 1543/06, § 66-68, ECHR 2007; See also Kudrevičius and others v. Lithuania cited above at n47, at § 100.

Examples of surveillance deployed after a protest



- **Police databases:** In the aftermath of protests or assemblies, police and/or law enforcement agencies often retain information gathered in the context of managing or facilitating a protest. This information can then be collated into databases and integrated with other forms of intelligence. Rules, guidelines, and information around how these databases are maintained and accessed are rare or inaccessible, and often left to the discretion of government agencies.
- **Predictive policing:** this is best understood as a form of "further processing" after law enforcement have built up databases about activists or people who have attended a protest. Predictive policing relies on programs which work "by feeding historic policing data through computer algorithms." The efficacy of predictive policing technology is heavily reliant on the quality, strength, and accuracy of the underlying data. PI has previously highlighted that, depending on the historic data that the police are using, these tools can be "incomplete or biased, leading to a 'feedback loop' sending officers to communities that are already unfairly over-policed". Police may use predictive policing technology to aggregate information that has been collected through surveillance technologies such as SOCMINT, IMSI catchers, or CCTV, and create "watchlists" for heightened surveillance and data collection. When it is used to target activists and protesters simply for attending multiple protests or for being organisers, it has the potential to deter people from exercising their right to freedom of assembly.

102 See for example, evidence from interviews with senior police in the UK in, Lina Dencik, Arne Hintz and Zoe Carey, "Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom" in New Media and Society, Vol. 20(4) 1443-1540 (2018) at page 1440.

103 Privacy International, "How predictive policing can be used at protests", 5 May 2021, accessed online: https://privacyinternational.org/explainer/4501/how-predictive-policing-can-be-used-protests

104 bid.

In the UK, a police database known as the "Extremism database" within the National Public Order Intelligence Unit held vast amounts of data about protesters and activists collected through covert and overt surveillance. It was maintained and used for the purposes of managing "public order issues".[105] However, after a series of allegations[106] and independent investigations deeply, disturbing intelligence gathering techniques by undercover police officers infiltrating more than 1,000 activist groups where brought to light. This included undercover agents entering into long-term sexual relationships with activists/ protesters – in some instances parenting children with them. Additionally, this included authorising under-cover agents to gather "tactical intelligence" about a family-run campaign group seeking justice for the murder of Stephen Lawrence – a black teenager who was killed in a racially motivated attack in 1993.[107] It also went as far as police conducting "extensive information gathering on schoolchildren perceived to have left-wing political sympathies, including regular reporting on their location, interests and perceived sexual orientation."[108] As a result of numerous allegations of systemic abuse by undercover policing units contributing this database over 40 years, a national inquiry investigating the way in which police gathered and managed this intelligence is ongoing.[109]

In the US, in the aftermath of the murder of George Floyd the MIT Technology Review reported that police in Minnesota allegedly built "a watch list…that includes photos and personal information identifying journalist and other

105 Her Majesty's Inspectorate of Constabulary (HMIC), "A review of national police units which provide intelligence on criminality associated with protest", (2012), accessed online: https://netpol.org/wp-content/uploads/2019/04/HMRC-National-Review-Of-Police-Units-2012.pdf

106 BBC, "Deceived activist Kate Wilson wins tribunal against Met Police", 30 September 2021, accessed online: https://www.bbc.co.uk/news/uk-england-nottinghamshire-58749590 See also, BBC Interview with Donna McLean, "Spy cops: 'He had two families and he had two lives.'", 7 February 2022, accessed online: https://www.bbc.co.uk/programmes/p0bmncbq

107 The UK Home Office, "Independent report: Stephen Lawrence independent review (The Ellison Review)", 6 March 2014, accessible online: https://www.gov.uk/government/publications/stephen-lawrence-independent-review

108 Dominic Glover, "Undercover policing inquiry exposes scale of British surveillance", 13 May 2022, Courthouse News Service, accessible online: https://www.courthousenews.com/undercover-policing-inquiry-exposes-scale-of-british-surveillance/

109 Dominic Casciani, "What is the Undercover Policing Inquiry?" 2 November 2020, BBC News, accessible online: https://www.bbc.co.uk/news/uk-54753627

people doing nothing more than exercising their constitutional rights."[110] The same investigative report also stated that police in Minnesota "used a real-time data-sharing tool called Intrepid Response, which was sold on a subscription basis by AT&T [one of the largest telecommunications companies in the US]…at the press of a button, images, videos (including footage captured by drones), geo-locations from team members and targets and other data can be instantly shared between field teams and command centre staff."[111] Notably, this included photos and information about journalists covering the protests.

110 Tate Ryan-Mosely & Sam Richards, "The secret police: Cops built a shadowy surveillance machine in Minnesota after George Floyd's murder", 3 March 2022, MIT Technology Review, accessible online: https://www.technologyreview.com/2022/03/03/1046676/police-surveillance-minnesota-george-floyd/.

111 ibid.

Applying the legal standards

Firstly, we must consider what consequences flow from the existence of a database which records personal, including sensitive, information about protesters in various contexts. Secondly, it is important to highlight the limits of predictive policing and its potential impact on individuals' human rights. Therefore, we will apply the general legal standards which we are advocating for and attempt to expand on them in the context of surveillance after a protest.

The #MeToo movement in India gained strength when women started sharing their testimonies of sexual harassment, abuse, and rape online and within private groups. Fundamental to the strength of the movement was the ability of women to share their stories anonymously. For example, a former employee of India's Supreme Court spoke out anonymously accusing India's then chief justice Ranjan Gogoi of sexual misconduct. This sparked a series of protests outside the Supreme Court and police stations, during which dozens of women were reportedly arrested.[112] We will outline a hypothetical scenario in order to illustrate the dangers of unregulated intelligence databases gathering information about protest movements: if, during these series of protests, the police found out the name of every woman who attended the protests, and built a database with this information, it could easily be linked with other personal data which is routinely held by various government agencies (e.g. data about residents/citizens/public employees). If personal data about protesters is retained and later, linked with data held by other government agencies, any protester who (a) had chosen to exercise her right to freedom of assembly and take part in the protests and (b)had also shared testimony anonymously could easily be identified, thereby undermining the safety that many survivors rely on to share their testimonies of harassment. Regardless of whether or not this information was leaked immediately, its mere existence, especially for an unlimited period of time creates a risk that it will be accessed, subjected to a breach, or shared. This can have serious consequences for activists at risk of retaliation for their political views or further harassment.

112 Michael Safi, "India's #MeToo backlash: accusers battle intimidation, threats, and lawsuits", 14 May 2019, The Guardian, accessed online: https://www.theguardian.com/world/2019/may/14/indias-metoo-backlash-accusers-battle-intimidation-threats-and-lawsuits

> **Police databases which retain vast amounts of personal data about protesters for unlimited periods of time, for the broad purposes of policing protests are incompatible with the right to freedom of assembly.**

Without robust restrictions and oversight on the type of data that can lawfully be retained, the purposes for which such data should be retained and the period for which it should be held, these databases may cause protesters to be subjected to hidden sanctions such as profiling, discrimination – and in some contexts, persecution. These hidden sanctions have the potential of chilling the exercise of the right to protest in order to avoid profiling by the police or law enforcement.

> **As such, a failure to implement legal restrictions on the retention and processing of personal data about protesters amounts to a breach of states' positive obligation secure the effective enjoyment of freedom of assembly.**

Therefore, in the absence of individualised reasonable suspicion of the commission of a serious crime, it is unlawful to retain protesters' personal data merely because they participated in a protest. Any personal data collected incidentally must be deleted without undue delay. For example, where police have a limited power to collect and retain information about individuals involved in protest movements for a legitimate purpose, such as organisers contact details to facilitate the exercise of the right to protest, personal data should be kept in a secure manner (for example, it should be anonymised, encrypted at rest and there should be clear access limitation and control).

> **Additionally, predictive policing should never be deployed at protests and cannot be used as a blanket justification to collect and retain personal data about protesters without limitation.**

Using databases to inform predictive policing technologies at protests poses serious risks in contexts where law enforcement has historically engaged in discrimination and/or persecution of certain groups or minorities on the basis

of their identity. By creating this risk for people who are exercising their right to protest, law enforcement agencies are imposing hidden sanctions on people merely for exercising their fundamental rights, as well as discriminating against particular groups.

Predictive policing as a method of policing in the context of protest policing has been described as "part of a shift from 'negotiated management', in which active cooperation between police and protesters is encouraged…to a strategy of 'strategic incapacitation' characterised by the goals of 'securitising society' and isolating or neutralising the sources of potentially disruptive actions or events."[113] **In this context, police use a variety of intelligence and surveillance to monitor risks and attempt to "predict (and control) the future".[114]**

The fundamental problem with using intelligence as data points to be 'fed' into computational processing which is either algorithmic (and therefore incorporates the logic of probability) or reliant on artificial intelligence, is that the data is collected and processed by humans and the software is developed by humans: thus, human bias, ideology, and judgment is necessarily reproduced in the software's output and therefore, "the social context of data generation is crucial for its interpretation".[115]

Another important issue with 'predictive policing' which has been highlighted by researchers is that risk which can be read from intelligence information or bigdata does not necessarily translate into a crime or breach of public order. Therefore, if police are acting on information which is potentially biased while at the same time ostensibly showing that certain risks are 'probable' "this can become conducive to an environment of over-intervention by the police."[116] As has already been argued by the House of Lords Justice and Home Affairs Committee in the UK, as artificial intelligence and algorithmic processing becomes a core feature of policing, "a national body should be established to

113 Lina Dencik, Arne Hintz and Zoe Carey, "Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom" in New Media and Society, Vol. 20(4) 1443-1540 (2018) at page 1436.

114 ibid.

115 ibid.

116 ibid., at page 1446.

set strict scientific, validity and quality standards to certify new technological solutions against those standards."[117] Additionally, any surveillance or policing tool deployed at protests which uses computational cognition must be subjected to qualitative testing and impact assessments by a wide variety of stakeholders before deployment at protests.

Arguments which present limitations on surveillance and data retention as conflicting with security and public safety at protests elide the fact that law enforcement, riot police, and people in positions of power may themselves pose a risk to the security and safety of particular groups of people who are seeking to use their right to freedom of assembly to demand greater equality or progress their rights against racist or oppressive institutions. Examples of nonviolent protest movements which faced hostility and abuse from police and law enforcement are plenty – from the movement against apartheid in South Africa, to the civil rights movements in the UK and the US.

117 House of Lords Justice and Home Affairs Committee, "Technology rules? The advent of new technologies in the justice system," 1st report of Session 2021-22, 30 March 2022, at page 4.

VI. CONCLUSION

It is legitimate for democratically elected governments to use new technologies to protect the public. However, mass surveillance which is generalised, secretive and not subjected to legal oversight mechanisms erodes our rights to freedom of assembly, association, expression, and privacy.

In 2022, the UN High Commissioner for Human Rights highlighted that "the widespread monitoring of public spaces"[118] is a trend which poses serious risks to human rights. Our report builds on recommendations that have repeatedly been delineated by international human rights standard-setting bodies across the UN. As such, we agree that - as a basic starting point –states should "avoid general privacy-intrusive monitoring of public spaces and ensure that all public surveillance mechanisms are strictly necessary and proportionate for achieving important legitimate objectives."[119] We have used this report to build on this starting point and to advocate for safeguards that specifically protect the rights to privacy and freedom of assembly, before, during and after protests take place.

Applying the framework of international human rights law to protest surveillance is necessary to avoid arbitrary and abusive interferences with the right to protest through surveillance. **Our report highlights that the consequences which flow from unrestricted protest surveillance amount to sanctions which unlawfully interfere with individuals' rights to privacy and freedom of assembly. This underpins and urgent need to impose legal restrictions on protest surveillance.**

118 n 31.

119 Ibid. at para 57(d).

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).