European Court of Human Rights

***Jakub Smoleń v Poland*, Application No 40387/20 and**
***Fundacja Greenpeace Polska v Poland,* Application No 40754/20**

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL

Introduction and summary of intervention

1. This intervention is submitted by Privacy International (PI) ('the Intervener') pursuant to leave granted by the President of the Section in accordance with Rule 44(3) of the Rules of the Court. PI is a human rights organization that researches and advocates globally against government and corporate abuses of data and technology.

2. This submission aims to contribute to the development of this Court's jurisprudence under Article 8 of the European Convention on Human Rights (the "Convention"), concerning secret surveillance measures deployed against human rights defenders and activists. The technologies that underpin these covert surveillance measures can afford the state unprecedented insights into the private lives of anyone who is monitored. Consequently, secret surveillance mechanisms can impede the ability of human rights defenders, activists, and journalists to carry out their roles in democratic societies.

3. This intervention will make four core submissions. First, we argue that there should be a legal presumption against subjecting human rights defenders to surveillance on the sole basis of their roles and/or membership in activist and civil society groups. Second, we argue that certain intrusive surveillance technologies should not be used to monitor human rights defenders and we propose some ways in which these technologies should be regulated. Thirdly, we submit that covert surveillance measures must be subject to a number of enhanced safeguards in order to comply with Article 8 of the Convention. Finally, we provide an analysis of when covert surveillance can be said to be necessary for the purposes of Article 8(2) of the Convention.

1. The case for a presumption against subjecting human rights defenders to surveillance

4. The Intervener submits that secret surveillance programmes dramatically undermine the protection of human rights defenders, including climate activists and individuals participating in protest movements. Such programmes inhibit their ability to pursue legitimate actions, including the promotion and protection of human rights, defending the environment and organising protests. Therefore, these surveillance measures constitute a serious interference with the right to privacy of activists and human rights defenders and should not be permitted. Surveillance measures endanger their public watchdog function by undermining the way in which they operate. Yet in the past years surveillance against climate activists has emerged as a concerning issue with significant implications as is attested by reports and resolutions by multiple human rights bodies, including the Human Rights Commissioner of the Council of Europe, the UN Human Rights Council, and others.[1]

[1] Commissioner for Human Rights, Council of Europe, "Highly intrusive spyware threatens the essence of human rights", Comment, 27 January 2023, https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-

5. The UN Special Rapporteur on Assembly has noted in his report on climate justice:

> Extensive surveillance by law enforcement is another result of the criminalization of environmental protesters and organizations. Such surveillance provides a channel through which the authorities can obtain information to later be used in thwarting protests and advocacy campaigns. The Special Rapporteur has received reports of individuals being filmed or photographed without their consent at climate protests. Such surveillance creates a chilling effect which may deter others from participating in assemblies or joining organizations for the purpose of pursuing climate justice.[2]

6. In 2021, PI conducted a survey aimed at climate activists and environmental defenders with the purpose of understanding their perception and experiences of surveillance.[3] The findings of the survey shed light on climate activists' own awareness of their surveillance risks. More than half of the respondents felt that they had been subjected to surveillance, with a similar percentage stating that they believed that it had occurred in the ordinary course of their activism. Notably, nearly 60% of respondents highlighted that they suspected that they had been surveilled by way of social media monitoring.[4] One third stated that they feared or thought about surveillance in the context of their activism. Further, over a third stated that they assumed that they were surveilled, on account of this being a regular practice. Of all respondents who reported surveillance incidents to law enforcement, or state oversight and human rights monitoring bodies, nearly a fifth stated that the relevant authorities took no action after the complaint was made.

7. Such practices curtail fundamental rights such as privacy, as well as the freedoms of expression and peaceful assembly, thereby impeding democratic participation and inhibiting the pursuit of environmental justice.[5] The ability of intelligence and security agencies to use their surveillance powers and capabilities covertly to surveil non-governmental organisations, activists and other civil society members has a profound chilling effect on the exercise of their role as a public watchdog.[6] If civil society organisations and activists are to perform their public watchdog function, the importance of which this Court has recognized,[7] they must be able, in a similar way to journalists,

---

human-rights?redirect=%2Fen%2Fweb%2Fcommissioner%2Fhuman-rights-defenders (hereinafter Commissioner for Human Rights 2023 Comment); Recognizing the Contribution of Environmental Human Rights Defenders to the Enjoyment of Human Rights, Environmental Protection and Sustainable Development, UN HRC Res 40/11 (20 March 2019) operative paras 2ff (hereinafter UNHRC Res 40/11 (2019)); OHCHR, Human Rights Defenders: Protecting the Right to Defend Human Rights, Fact Sheet No 29 2004, p 12; Right to Privacy in the Digital Age, UNHRC Res 48/4 (7 October 2021) preambular para 28 (hereinafter UNHRC Res 48/4).

[2] Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association on the exercise of the rights to freedom of peaceful assembly and of association as essential to advancing climate justice, A/76/22 (23 July 2021), para 34.

[3] Privacy International, "How to avoid social media monitoring: A Guide for Climate Activists" (2022), https://privacyinternational.org/long-read/5000/how-avoid-social-media-monitoring-guide-climate-activists.

[4] PI, 'How social media monitoring can be used at a protest' (2021) https://privacyinternational.org/explainer/4509/how-social-media-monitoring-can-be-used-protest.

[5] UNHRC Res 40/11 (2019), note 1, operative para 3; UN Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (article 21), CCPR/C/GC/37 (17 September 2020) (hereinafter General Comment 37 (2020)); Report of the United Nations High Commissioner for Human Rights on the impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, A/HRC/44/24 (25 June 2020) (hereinafter A/HRC/44/24 (2020)).

[6] Report of the Special Rapporteur on the Situation of Human Rights Defenders, Human Rights Defenders Operating in Conflict and Post-Conflict Situations, A/HRC/43/51 (30 December 2019) para 34; Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Impact of Measures to Address Terrorism and Violent Extremism on Civic Space and the Rights of Civil Society Actors and Human Rights Defenders, UN Doc A/HRC/40/52 (1 March 2019) para 27.

[7] ECtHR, *Szabó and Vissy v Hungary,* App No 37138/14, Judgment, 12 January 2016, para 38; ECtHR, *Vides Aizsardzības Klubs v Latvia*, App No 57829/00, Judgment, 27 May 2004, para 42. CJEU, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs ao*, Case C-623/17, Judgment, 6 October 2020, para 72.

to guarantee the anonymity of their sources and the confidentiality of their communications and movements.

8. The UN Human Rights Council has called upon states to:

> refrain from the use of surveillance technologies in a manner that is not compliant with international human rights obligations, including when used against journalists and human rights defenders, and to take specific actions to protect against violations of the right to privacy, including by regulating the sale, transfer, use and export of surveillance technologies.[8]

9. Yet the knowledge that intelligence and security services may without accountability intercept their communications or track their location puts at risk the ability of human rights defenders to collect essential information and to organise movements. Increasingly, examples that have come to light demonstrate the causal connection between the interference with the right to privacy and the enjoyment of other human rights, including the right to life.[9] For the above reasons, the Intervener submits that the surveillance of human rights defenders on the sole basis of their role and/or membership of activist and civil society groups is likely to fall outside the scope of lawful surveillance. This is because as stated above at paragraph 4 such surveillance targets legitimate and lawful conduct in contravention of the requirements set in Article 8(2) and has a chilling impact on the exercise of fundamental human rights. There should, therefore, be a presumption that surveillance of human rights defenders, including climate activists on the mere basis of their roles and membership of civil society groups, is unlawful.

10. Such a presumption is likely to inhibit law enforcement and security services from unlawfully targeting human rights defenders with covert surveillance. This is because a presumption against surveillance would necessitate consideration of the conduct of the individual concerned, which as set out below is required pursuant to the principle of necessity for the purposes of Article 8(2) of the Convention. Individualised consideration would in turn likely embed adherence to other human rights safeguards in the use of surveillance in investigations, including the requirement for reasonable suspicion that an individual has committed a serious crime and/or that they present a grave threat to national security.

11. We submit that a reasonable suspicion requirement alongside the proposed presumption are necessary pre-conditions prior to the secret surveillance of human rights defenders, as they prevent arbitrary and indiscriminate surveillance. The presence of such reasonable suspicion has been deemed by this Court as critical to enable "the authorising authority to perform an appropriate proportionality test".[10]

12. In *Roman Zakharov*, the Grand Chamber held that the authorisation procedure:

> must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.[11]

[8] UNHRC Res 48/4 (2021), note 1, operative para 6(k). See also UN Human Rights Committee, Concluding Observations on the Fourth Periodic Report of Paraguay, CCPR/C/PRY/CO/4 (20 August 2019) para 37.
[9] Report of the Special Rapporteur on the situation of human rights defenders on Final warning: death threats and killings of human rights defenders, A/HRC/46/35 (24 December 2020) paras 55 & 77.
[10] *Szabó ao v Hungary,* para 71.
[11] ECtHR, *Roman Zakharov v Russia*, App No 47143/06, Grand Chamber, Judgment, 4 December 2015, para 260.

2. Secret surveillance with very intrusive technologies and the need for regulation

13. The Intervener submits that the ability to ensure compliance with human rights obligations is today further challenged by modern technologies enhancing state authorities' surveillance capabilities. State authorities have access to a wide array of technologies that they can use to covertly surveil their targets. Advanced surveillance systems, such as drones, GPS trackers, communication interception technologies, facial recognition systems, and data aggregation tools, have become increasingly sophisticated and pervasive. Through the integration of artificial intelligence and machine learning algorithms, surveillance capabilities have grown even more intrusive, allowing for the automated identification, profiling, and monitoring of individuals on a massive scale.

14. As such, these technologies have significantly expanded the scope and intrusiveness of monitoring activities by state authorities. The vast volume of personal data collected frequently includes facial images and other sensitive data that can reveal a target's political opinion, religious belief, health conditions, sexual orientation and gender identity. The intrusiveness of the intelligence that can be obtained through these mechanisms is exemplified when one closely considers the specific surveillance capabilities of technologies at the disposal of law enforcement and intelligence services.

i. Examples of some of the relevant technologies in question

15. **Drones**: In the past years, the use of drone technology for domestic law enforcement operations has dramatically increased.[12] The use of drones is particularly concerning as they are equipped with progressively more intrusive data collection tools. Drones used by domestic law enforcement agencies were initially equipped with cameras only, but today are "routinely equipped with enhanced features such as thermal and night-vision imaging, automatic target tracking, loudspeakers and spotlights",[13] as well as facial recognition technologies.

16. Drones can therefore record details of an individual's every move and collect sensitive biometric data. They infringe the ability of people to remain anonymous in public places. Anonymity enables human rights defenders and activists to communicate confidentially and securely, which is vital in order to plan, organise, and participate in protests.[14] Individuals rely on the anonymity of the crowd to protect themselves against retribution, particularly in contexts where any form of dissent is suppressed. This is no longer an option when drones with the above surveillance capabilities are in place.

17. In addition, due to their mobile nature it is very difficult to track their movements and have a clear understanding on what areas they surveil and why. These are questions essential to determine the lawfulness of the legal framework that regulates them and their use. The lack of transparency

[12] As the UN Special Rapporteur highlighted: "drone technology has followed the same well-worn path from the battlefield to the home front". Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism, A/HRC/52/39 (1 March 2023) para 31 (hereinafter A/HRC/52/39).
[13] *ibid*, para 32.
[14] General Comment 37 (2020), note 5; A/HRC/44/24 (2020), note 5.

surrounding their use contributes to a climate of fear, which has "a chilling effect on demonstrations, as people fear subsequent reprisals for planning or participating in protests".[15]

18. The Intervener submits that drones, especially when equipped with surveillance capabilities such as facial recognition technologies, should never be used to identify human rights defenders, including climate activists and those participating in protests. This is in line with recommendations by human rights bodies, where the recourse to facial recognition technology during peaceful protests could never meet the test of necessity and proportionality, given its intrusiveness and serious chilling effects has been questioned.[16]

19. The UN High Commissioner for Human Rights and the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association have called on states to refrain from using facial recognition technologies to identify those peacefully participating in an assembly.[17]

20. **GPS car trackers**: A Global Positioning System (GPS) car tracker enables the state authorities to track the location of a vehicle in real time. Anyone who has used a GPS-based smartphone app, such as Google Maps, will have seen something very similar to how GPS tracker work: the app will record their location on the Earth's surface, from which it can also work out their direction of travel and speed.[18] "GPS technology provides law enforcement with a powerful and inexpensive method of tracking individuals over an extensive period of time and an unlimited expanse of space as they traverse public and private areas."[19] They may be able to follow past and current movements of a vehicle, as well as confirm meetings with other tracked persons.[20]

21. This is an invasive technology that can track someone's movements thereby potentially exposing sensitive information, such as political meetings or information relevant to the organisation of protests. This Court has recognised that the use of GPS trackers amounts to an interference with the right to privacy.[21]

22. Similarly, the US Supreme Court has recognised that installing a tracking device on a car and monitoring its movements constitutes an interference with the right to privacy.[22] The US's highest court concluded that their use is so intrusive that it should be prohibited unless authorized by a

---

[15] A/HRC/44/24 (2020), note 5, para 29. The UN Special Rapporteur's recent report underlined:

> She underscores again that this is consistent with the broader trend she identifies of the short-lived exceptional use of certain technologies and their rapid reinvention as ordinary State practice. In addition to the obvious implications for privacy, freedom of assembly, freedom of expression and the right to participate in political affairs, the use of drones coupled with the coercive power of the police brings the issues of arbitrary detention, the liberty and security of the person, and the right to life into play. A/HRC/52/39, note 12, para 34.

[16] European Union's Fundamental Rights Agency, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", FRA Focus, 2019, p 34, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf; A/HRC/44/24 (2020), note 5, paras 61 & 75.

[17] A/HRC/44/24 (2020), note 2, para 53(h); Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, Access to Justice as an Integral Element of the Protection of Rights to Freedom of Peaceful Assembly and Association, A/HRC/47/24 (12 May 2021) para 57.

[18] PI, "Electronic monitoring using GPS tags: a tech primer" (2022) https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer.

[19] Brief of the American Civil Liberties Union and ACLU of the Nation's Capital as Amici Curiae in support of respondent in case *U.S. v Jones*, No 10-1259, Supreme Court of the United States.

[20] *ibid*.

[21] ECtHR, *Uzun v Germany*, App No 35623/05, Judgment, 2 September 2010.

[22] The government in this case placed a GPS device on the defendant's car and tracked his movements for a month without a search warrant.

court via a warrant on the basis that there was probable cause to believe that criminal activity was taking place.[23]

23. The use of each of these technologies on their own to track and monitor human rights defenders, such as climate activists, constitutes a serious interference with their right to privacy. Their cumulative use introduces a new degree of unprecedented surveillance creating an atmosphere of fear under the weight of constant and relentless surveillance that crushes activism and stifles dissent, undermining core democratic principles and the rule of law.[24]

24. The Intervener submits that state authorities do not have a *carte blanche* to indiscriminately use any means and methods at their disposal. This Court has repeatedly affirmed that while the state authorities enjoy a certain margin of appreciation in relation to the secret surveillance measures, this margin is subject to European supervision embracing both legislation and judicial decisions applying it.[25] Therefore, their deployment needs to be assessed both in relation to the quality of the law regulating their use and the specific circumstances in each individual case.

25. Otherwise as this Court has highlighted:

> 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 democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse.[26]

ii. The regulation of secret surveillance mechanisms

26. In respect of the regulation of intrusive surveillance technologies, there needs to be a clear, foreseeable, and adequately accessible legal framework regulating their use. In the case of *Uzun v Germany*, the legal framework allowed the use of GPS trackers for investigations of serious crime and in the absence of other less intrusive measures.[27]

27. With regard to the foreseeability criterion, in *Ben Faiza v France* the covert GPS monitoring of a car in a similar criminal investigation took place under a general power for investigating officials to take whatever intelligence-gathering steps they deemed useful in order to establish the facts of the case. This provision was held by this Court to be insufficiently precise as it did not provide sufficient clarity in relation to the extent and manner in which officials were permitted to exercise their discretion[28]. The requirement for foreseeability was deemed to be all the more important given the highly intrusive nature of real time locational tracking.

28. As per this Court's jurisprudence, the secret surveillance of an individual must have some basis in domestic law and be compatible with the rule of law.[29] This Court has particularly highlighted that:

---

[23] US Surpeme Court, *United States v Jones* (2012), 565 U.S. 400 (2012).
[24] "The use of spyware has a chilling effect on other human rights and fundamental freedoms, including freedom of expression and public participation." Commissioner for Human Rights 2023 Comment, note 1. Also Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/41/35 (28 May 2019) para 26.
[25] ECtHR, *Klass and Others v Germany*, App No 5029/71, Judgment, 6 September 1978, para 50.
[26] ECtHR, *Big Brother Watch and Others v UK,* App nos 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment, 25 May 2021, para 339; *Roman Zakharov v Russia* [GC], para 232.
[27] *Uzun v Germany*.
[28] ECtHR, *Ben Faiza v France*, App No 31446/12, Judgment, 8 February 2018.
[29] *Roman Zakharov v Russia* [GC], para 227; *Szabó ao v Hungary*, para 54.

> [i]n the special context of secret measures of surveillance, […] "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, **especially as the technology available for use is continually becoming more sophisticated**.[30]

29. Thus, the ability of state authorities to deploy particularly intrusive technologies in targeted secret surveillance operations should be strictly limited to exclude the targeting of human rights defenders. There should also be transparency regarding the capabilities each of the tools are equipped with, and their use should be subject to judicial control and robust safeguards.

3. Enhanced safeguards necessary to ensure compliance with requirements of Article 8 and protect human rights defenders

30. The Intervener submits that for Convention rights to remain effective, the particularly serious deterrent effect of secret surveillance measures on civil society organisations and activists calls at the very least for enhanced safeguards against surveillance measures. These enhanced safeguards become imperative particularly when secret surveillance measures involve extreme and unprecedented intrusions to privacy.

i. Any interference with the right to privacy should be subject to authorisation by an independent judicial authority

31. Intrusive, secret surveillance measures, like those at issue here, should be subject to authorisation by an independent judicial authority. In *Roman Zakharov*, this Court held that such authorisation could be given by a non-judicial authority "provided that the authority is sufficiently independent from the executive."[31] The Court repeated the principles in *Szabó ao*:

> in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exceptions, warranting close scrutiny ... supervision by a politically responsible member of the executive, such as the Minister for Justice, does not provide the necessary guarantees.[32]

It added that independent, "preferably judicial," review "reinforc[es] citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained".[33]

[30] *Big Brother Watch ao v UK* [GC], para 333; *Roman Zakharov v Russia* [GC], para 229 (emphasis added).
[31] *ibid*, para 258.
[32] *Szabó ao v Hungary,* para 77.
[33] *ibid,* paras 77-79.

32. The same approach was taken by the Court of Justice of the European Union in relation to intrusive surveillance practices.[34] This requirement for independent authorisation has been further confirmed by international human rights bodies.[35]

33. The Intervener submits that a system of prior judicial authorisation would minimise unnecessary or disproportionate interferences with privacy. A limited post-authorisation oversight regime that only examines a restricted breadth of information is not sufficient. This is particularly the case when there is no complaint mechanism available to challenge such interferences.

ii. Any interference with the right to privacy should be subject to independent and effective oversight

34. State surveillance, including targeted covert surveillance, should be subject to independent, effective, adequately resourced and impartial domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability.[36]

35. As the UN High Commissioner for Human Rights noted, effective oversight should ensure that:

> Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.[37]

36. The Intervener submits that effective oversight cannot be limited to an automatic and superficial review of the reported interferences, without the ability to review all available information and authority to issue binding decisions.

iii. Subjects' notification (even if post facto*) and effective remedies*

37. There is an increasing consensus that notification requirements are necessary to enable individuals who are subjected to secret surveillance measures to challenge unlawful surveillance decisions. This Court has consistently recognised the importance of notification as both an adequate safeguard against the abuse of surveillance powers under Article 8 and as part of the right to an effective

[34] CJEU, Joined cases *Tele2 Sverige AB v Post-och telestyrelse*n and *Secretary of State for the Home Department v Tom Watson*, Cases Nos. C–203/15 and C–698/15, Judgment, 21 December 2016, para 120; CJEU, Joined cases *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others*, Cases Nos. C-293/12 and C-594-12, Judgment, 8 April 2014, para 62.

[35] UN Human Rights Committee, Concluding observations on the fifth periodic report of Belarus, UN Doc. CCPR/C/BLR/CO/5 (22 November 2018); UN OHCHR, Report on the right to privacy in the digital age, A/HRC/39/29 (3 August 2018) (hereinafter A/HRC/39/29); CoE ComHR, "Memorandum on surveillance and oversight mechanisms in the UK", CommDH(2016)20, 17 May 2016, para 28 (referring to the Venice Commission's Report on Democratic Oversight (2007)).

[36] *ibid.* See also The Right to Privacy in the Digital Age, UN GA Res 73/179 (17 December 2018); *Big Brother Watch ao v UK* [GC], para 346.

[37] A/HRC/39/29, note 36, para 40. See also *Association for European Integration and Human Rights ao v Bulgaria*, para 85.

remedy under Article 13.[38] In *Weber,* the Court noted that there is "in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".[39]

38. In its judgment in *Schrems*, the CJEU added that:

> [a]ccording to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.[40]

39. International human rights bodies and experts, including the UN High Commissioner for Human Rights, have repeatedly underlined the significance of notification to ensure the presence of an effective remedy in response to violations of the right to privacy.[41]

40. In light of the above, we submit that it is key that this Court concludes that notification is a necessary safeguard in cases of secret surveillance operations targeting human rights defenders. Whilst notification of surveillance is not an absolute right in the sense that it should operate without restrictions, any restriction on notification should be strictly limited, i.e. it should only be delayed where it would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life.

41. As to when, practicably, an individual should be notified, this Court has acknowledged that "as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned".[42] Any such delay in notification, moreover, must be judicially authorised and subject to continuing judicial oversight. The burden must be on the government to satisfy an independent and impartial tribunal that continued non-notification is both necessary for a legitimate aim and proportionate.[43]

---

[38] *Szabó ao v Hungary,* para 86. See also, *Association for European Integration and Human Rights ao v Bulgaria,* para 91.

[39] ECtHR, *Weber and Savaria v Germany,* App No 54934/00, Decision, 29 June 2006, para 135.

[40] CJEU, Data Protection Commissioner v Facebook Ireland and Schrems (Schrems II), Case C-311/18, Judgment, 16 July 2020, para 187, see also CJEU, Joined cases *Tele2/Watson* cases, note 28, para 121.

[41] This Court has further highlighted:

> the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, cited above, § 57, and Weber and Saravia, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also Kennedy, cited above, § 167). *Big Brother Watch ao v UK* [GC], para 337.

UN OHCHR, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014, para 47; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 (17 April 2013) para 82; Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression, 21 June 2013, para 5.

[42] *Weber ao v Germany,* para 135. Further, this Court has, in past cases, taken note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without their knowledge, and unless the data is deleted, they should be informed, where practicable, that information is held about them as soon as the object of the police activities is no longer likely to be prejudiced. *Roman Zakharov v Russia* [GC], para 287.

[43] On a comparative analysis of notifications regimes in Council of Europe countries and beyond, see PI intervention in *Pietrzak ao v Poland* case before this Court (App Nos 72038/17 and 25237/18) https://privacyinternational.org/legal-action/pietrzak-and-others-v-poland

4. Secret surveillance measures should be necessary for the obtaining of vital intelligence in an individual operation

42. The Intervener submits the quality of the measures taken pursuant to the law must also be necessary in a democratic society and the use of these tools should be assessed against the particular circumstances of the case. The Intervener submits that the state authorities need to adjust the means and methods used in each specific case, incorporating a consideration of what measure was necessary and what impact its use could have.[44]

43. This Court has found in previous cases that the powers of secret surveillance of citizens, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.[45] The concept of "strict necessity", as clarified by this Court, requires that a measure of secret surveillance must, in general, be strictly necessary for the safeguarding of democratic institutions and, in particular, for the obtaining of vital intelligence in an individual operation. Otherwise, the authorities will have committed an "abuse".[46]

44. This Court has recognised that:

> the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[47]

45. The Intervener further submits that this assessment should take into account the severity of the interference with the right to privacy, including in relation to the specific means and methods used in a particular case to achieve the aim pursued. As this Court has concluded in a different case "a system should afford the possibility of an effective proportionality assessment of instances of restriction of an individual's rights".[48] It has also affirmed that in determining whether the impugned measures were "necessary in a democratic society", it will consider whether, in the light of the case as a whole, the reasons adduced to justify them were relevant and sufficient and whether the measures were proportionate to the legitimate aims pursued.[49]

46. The choice of means and methods of surveillance should be assessed on a case-by-case basis: balancing the extent of the intrusion against the specific benefit accruing to investigations

---

[44] As the Court has highlighted in other cases under Article 8, the proportionality assessment of the competing interests at stake and give consideration to the relevant rights secured by Article 8 ECtHR, *Liebscher v Austria*, App no 5434/17, Judgment, 6 April 2021, paras 64-69.

[45] *Szabó ao v Hungary*, paras 72-73.

[46] As this Court has underlined:

> given the **particular character of the interference in question** and **the potential of cutting-edge surveillance technologies to invade citizens' privacy**, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, **moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation**. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. *Szabó ao v Hungary*, para 73 (emphasis added). See also *Roman Zakharov v Russia* [GC], para 227; *Kennedy v UK*, para 130.

[47] ECtHR, *S and Marper v UK*, App nos 30562/04 and 30566/04, Judgment, 4 December 2008, para 112.

[48] *Liebscher v Austria*, para 61.

[49] ECtHR, *Z v Finland*, App No 22009/93, Judgment, 27 February 1997, para 94.

undertaken and taking into account the particular circumstances of the case, and the measure chosen must be "the least intrusive instrument among those which might achieve the desired result".[50] The cumulative use of a series of intrusive surveillance means and methods to target human rights defenders puts into question the extent to which these measures aim to intimidate and harass the targets.

47. In summary, the Intervener submits that in assessing the compliance of the state authorities with the standards of the Convention the Court should consider the specific circumstances of the case including:

    a. The secret nature of the surveillance operation;
    b. The position of the individuals and organisations against whom the measures are taken as human rights defenders; and
    c. The intrusiveness of the surveillance technologies.

48. There should be a presumption against the lawful of surveillance measures targeting human rights defenders. Further, due to their intrusive nature, state authorities should refrain from using certain surveillance technologies to surveil those participating in human rights movements and protests. Finally, surveillance technologies should be strictly regulated in relation to the conditions under which they can be used. There should be transparency regarding the capabilities with which each of the tools they use are equipped and their use should be subject to judicial control and robust safeguards.

Dr Ilia Siatitsa
Lawyer and Senior Legal Officer
Privacy International

Jonah Mendelsohn
Lawyer and Legal Officer
Privacy International

[50] UN Human Rights Committee, General Comment No 27 (67) Freedom of movement (article 12), CCPR/C/21/Rev.1/Add.9 (1 November 1999) para 14; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397 (23 September 2014) para 19.