

IN THE EUROPEAN COURT OF HUMAN RIGHTS

App No. 7256/25

BETWEEN:

MAKARIOS DROUSIOTIS

Applicant

and

CYPRUS

Respondent

WRITTEN COMMENTS OF THE THIRD-PARTY INTERVENER

9 July 2026

Introduction

1. These submissions are filed by Media Defence (the ‘Intervener’), pursuant to leave granted by the President of the Section in accordance with Rule 44 of the Rules of Court.¹
2. The applicant is a journalist and author whose investigations concern alleged corruption at the highest levels of government in Cyprus. He claims that the Cypriot authorities have subjected him to secret surveillance through interference with his electronic devices, and that this surveillance has been deployed to deter him from carrying out investigative journalism and to obtain access to sensitive information relating to his investigations.
3. The case engages fundamental questions about the compatibility of covert surveillance, and in particular spyware, with the rights guaranteed under Articles 8, 10, and 13 of the Convention. These submissions will focus on states’ use of spyware as a form of covert surveillance, and the challenges inherent in that context for the protection of press freedom. Surveillance technology is now routinely deployed against journalists whose work focuses on exposing corruption and other crimes in both the public and private sectors, with profound consequences for press freedom. State reliance on national security when deploying a tool which is designed for clandestine use has the potential to fatally undermine the safeguards that press freedom depends upon. It is against that backdrop that the Intervener makes the following submissions:
 - (i) the essential function of source confidentiality in enabling investigative journalism to serve its public watchdog role, and the obligations on states under Article 10 to protect that function;
 - (ii) the specific nature of spyware as a surveillance tool that, by circumventing end-to-end encryption and compromising the device itself rather than the communication channel, represents a qualitatively distinct form of surveillance requiring that any authorising legal framework satisfy an especially stringent standard of precision, foreseeability, and independent oversight under Articles 8 and 10 of the Convention;
 - (iii) the particular harm that covert surveillance inflicts on the freedom of the press, including its capacity to generate a severe chilling effect on investigative journalism irrespective of whether direct evidence of specific interception is available; and
 - (iv) the evidentiary difficulties that arise in cases of secret surveillance, and the implications of those difficulties for the assessment of victim status, the burden and standard of proof, and the effectiveness of domestic remedies.

¹ Letter dated 18 June 2026 received from the Court granting Media Defence leave to intervene. As stipulated in that letter, these submissions do not address the facts and merits of the case, addressing only the general principles applicable to the case.

Source confidentiality and the Article 10 obligations of states

4. The Court has consistently emphasised that the protection of journalistic sources is one of the cornerstones of press freedom, and the absence of such protection could deter journalistic sources from assisting the press in informing the public on matters of general interest.² Consequently, the press might be less able to fulfil its indispensable role as a ‘watchdog’ and its ability to provide accurate and reliable information might be impaired.³ The Court must therefore apply “special scrutiny” when considering restrictions on the confidentiality of journalistic sources and has made clear that interferences with those sources can only be justified where strict substantive and procedural guarantees are complied with.⁴
5. Spyware poses a distinct and heightened threat to this framework of protection. The absence of effective regulatory frameworks has resulted in the widespread use of spyware by states, with minimal safeguards governing its transfer or deployment. In a broad sense, this is eroding core human rights, including freedom of expression, press freedom, and privacy.⁵ Within the Council of Europe region, civil society organisations have documented the extensive use of spyware against journalists, politicians, and others, including - ⁶

in Italy, where journalists have been targeted by state actors.⁷ A parliamentary committee confirmed the state’s use of Paragon’s Graphite spyware, justified on national security grounds, while subsequent prosecutorial findings confirmed that journalists were also targeted;⁸

in Spain, where government critics have been targeted with spyware attributed to the state. A 2022 Citizen Lab investigation found that at least 65 individuals connected to the Catalan independence movement had been targeted with Pegasus and other spyware.⁹ Spain’s intelligence service later confirmed conducting

² ECtHR, *Goodwin v. the United Kingdom* [GC], App. no. 17488/90, 27 March 1996.

³ *Ibid.*, para 39.

⁴ ECtHR, *Sanoma Uitgevers B.V. v. the Netherlands* [GC], App. no. 38224/03, 14 September 2010, para 51.

⁵ Council of Europe, Information Society Department DGI (2022)04, *Pegasus Spyware and its Impact on Human Rights*, Tamar Kaldani and Zeev Prokopets, available at <https://edoc.coe.int/en/data-protection/11112-pegasus-spyware-and-its-impact-on-human-rights.html>

⁶ See Human Rights Watch, *Looking the Other Way: European Union Fails to Control Surveillance Exports* (12 May 2026), available at <https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights>

⁷ Amnesty International, *Italy: New case of journalist targeted with Graphite spyware confirms widespread use of unlawful surveillance* (13 June 2025), available at <https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/>

⁸ Civic Space Watch, *Italy: New cases of government use of spyware against journalists and activists* (23 October 2025), available at <https://civicspacewatch.eu/alert/italy-new-cases-of-government-use-of-spyware-against-journalists-and-activists/>

⁹ The Citizen Lab, *Would you click?*, available at <https://catalonia.citizenlab.ca/>

surveillance against 18 individuals with judicial authorisation from the Supreme Court;¹⁰

in Greece, where journalists and politicians have been targeted with spyware by the state. The ‘Predatorgate’ scandal confirmed that journalist Thanasis Koukakis was both wiretapped by the National Intelligence Service and infected with Predator spyware. Remarkably, Citizen Lab reported that the electronic device of a former member of the European Parliament was infected with Pegasus spyware while he was serving on the European Parliament committee investigating spyware use by states;¹¹ and

in Hungary and Poland, where spyware has been deployed against a range of targets considered hostile to the governments then in power, including journalists, while a report from the European Parliament describes Cyprus as “a popular destination for many Israeli spyware companies”¹² and highlights how spyware, including Pegasus, has been used extensively throughout the EU.¹³

6. These are flagrant examples of state violations of their negative obligations not to interfere with Article 8 and 10 rights, as well as their positive obligations to protect under those provisions. For journalists, those obligations are heightened.¹⁴ This Court has articulated the standards that must be adhered to when implementing surveillance operations: there must be a law that is clear, foreseeable and accessible, and where national security is relied upon as the legitimate aim, there must be a limit on the extent of the interference.¹⁵ The proportionality of any interference must be properly and independently assessed, including the necessity of surveillance, whether less intrusive means could achieve the same objective, whether sufficient safeguards are in place to prevent abuse, and whether the scope and volume of data collected is strictly

¹⁰ Assemblea, *The Spanish Intelligence Centre (CNI) admits to spying on two former ANC presidents with authorisation from the Supreme Court*, 2 December 2025, available at <https://int.assemblea.cat/news/the-spanish-intelligence-centre-cni-admits-to-spying-on-two-former-anc-presidents-with-authorisation-from-the-supreme-court/>

¹¹ Citizen Lab, *Espionage against the European Parliament* (3 July 2026), available at <https://citizenlab.ca/research/member-of-committee-investigating-spyware-hacked-with-pegasus/>. The hacking of Mr Kouloglou’s device took place between October 2022 and March 2023, demonstrating the difficulty in identifying spyware use as it happens.

¹² European Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware, Recommendation of 15 June 2023 (2023/2500(RSP)), P9_TA(2023)0244.

¹³ *Ibid.* See also Politico, “How Europe became the Wild West of Spyware” (25 October 2023), available at politico.eu/article/how-europe-became-wild-west-spyware/

¹⁴ See, for example, ECtHR, *Becker v. Norway*, App. no. 21272/12, para 76, 5 October 2017, where the Court notes that “protection afforded to journalists in respect of their right to keep their sources confidential is “two-fold, relating not only to the journalist, but also and in particular to the source who volunteers to assist the press in informing the public about matters of public interest.”

¹⁵ ECtHR, *Roman Zakharov v Russia*, [GC], App. no. 47143/06, para 303, ECHR 2015; ECtHR, *Weber and Saravia v Germany*, App. no. 54934/00, 29 June 2006, para 106.

limited to what is necessary to achieve the aim.¹⁶ In addition, an effective remedy must be available.¹⁷

7. The nature and extent of the threat that spyware poses to these obligations can only be properly assessed once the technical characteristics that distinguish it from more conventional surveillance are considered.

Spyware as a qualitatively distinct form of surveillance

8. Spyware represents a qualitatively different form of surveillance from the interception of communications that this Court has addressed in cases such as *Roman Zakharov*,¹⁸ and *Szabó and Vissy*.¹⁹ That difference is critical to the assessment of whether any legal framework can authorise the use of spyware in a manner compatible with the Convention.
9. Unlike conventional interception, which operates at the level of the communication channel and can in principle be limited to specific communications, spyware operates by compromising the device itself. Once a device is infected, the operator obtains total and largely indiscriminate access to its contents: all stored messages, contacts, emails, photographs, notes, browsing history, deleted files, passwords, and location data.²⁰ Many spyware products additionally enable real-time surveillance through the device's microphone, camera, and GPS, and some permit data on the device to be altered, deleted, or inserted. For example, NSO's 'Pegasus Product Description' document highlights and extols the virtues of: the extraction and ongoing collection of all data stored on or by an infected device; location tracking; interception and recording of voice calls; real-time interception and recording of sounds in the vicinity of the device by covert activation of the in-built microphone; and real-time interception and recording of images by covert activation of the in-built camera.²¹
10. A particularly significant feature of modern spyware is its capacity to circumvent end-to-end encryption. The primary means by which investigative journalists communicate with their sources is through encrypted messaging applications, precisely because end-to-end encryption provides a technical guarantee of confidentiality that supplements the legal protections afforded to journalistic sources.²² By compromising the device rather than the communication channel, spyware renders these technical protections entirely ineffective: the operator accesses

¹⁶ ECtHR, *Ekimdzhev and Others v. Bulgaria*, App. no. 70078/12, paras 321, 400 – 406, 11 January 2022

¹⁷ *Roman Zakharov v Russia*, cited above, paras 231 – 234; ECtHR, *Szabó and Vissy v. Hungary*, no. 37138/14, paras 56 – 57, 12 January 2016; ECtHR, *Big Brother Watch and Others v. United Kingdom* [GC] App. nos. 58170/13, 62322/14 and 24960/15, para 357.

¹⁸ ECtHR, *Roman Zakharov v Russia*, [GC], App. no. 47143/06, paras 7 – 14, ECHR 2015.

¹⁹ ECtHR, *Szabó and Vissy v. Hungary*, no. 37138/14, paras 8 – 14, 12 January 2016;

²⁰ See Amnesty International, *What is Spyware and What Can You Do to Stay Protected?* (December 2023); EPIC, *The Fight to Protect Our Phones – A Multi-Prong Approach to Spyware Reform* (November 2025).

²¹ NSO Group, *Pegasus Product Description*, available at <https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf>

²² Speech by the Commissioner for Human Rights, *Encryption in the Age of Surveillance* (26 September 2023), available at <https://www.coe.int/en/web/commissioner/-/encryption-in-the-age-of-surveillance>

the content of messages on the device itself, after decryption, without interacting with the communication channel at all.²³ This Court has held that measures requiring access to encrypted communications without sufficient safeguards impair the very essence of the right to respect for private life under Article 8 -

*Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field.*²⁴

11. The device-level takeover enabled by spyware represents an intrusion qualitatively more severe than mandated access to stored communications data and must therefore be assessed against an even more demanding legal standard.
12. A further essential feature of spyware is its covertness. Unlike the physical seizure of a device, which a target will immediately detect, or conventional interception of which a target may in due course become aware, spyware is specifically designed to leave no trace, to prevent detection, to operate invisibly for extended periods, and to be removed surreptitiously. This by-design undetectability has direct implications for the 'quality of law' requirements under Articles 8 and 10. In *Roman Zakharov*, the Court restated the six minimum safeguards that legislation governing secret surveillance must contain.²⁵ Applied to spyware, each of those safeguards requires reassessment and recalibration in order to assess whether they can be effective. The indiscriminate and total access that spyware permits makes it very difficult to impose limitations based on the nature of offences or the categories of data accessible. The covert and self-concealing nature of the technology makes independent oversight, notification, and ex post review structurally more difficult to implement. In addition, the involvement of private commercial spyware entities, who may retain access to data collected and over whom the authorising state might not exercise direct control,²⁶ introduces accountability gaps that existing frameworks for communication interception do not address.²⁷
13. Because spyware such as Pegasus is engineered to operate covertly and erase its traces, its use cannot be independently audited. There is therefore no means of verifying whether a particular deployment complied with the safeguards this Court requires at each stage of a surveillance operation, whether it was used to target individuals for

²³ ECtHR, *Podchasov v. Russia*, App. no. 33696/19, para 77, 13 February 2024.

²⁴ *Ibid.*

²⁵ *Roman Zakharov*, cited above, paras 231 – 234.

²⁶ The Record, *Testimony from NSO Group raises questions about its culpability for spyware abuses*, 19 November 2024, available at <https://therecord.media/nso-group-whatsapp-case-documents>

²⁷ See, for example, Privacy International, *Operating from the Shadows: Inside NSO Group's Corporate Structure*, 22 July 2021, available at <https://privacyinternational.org/press-release/4596/press-note-release-report-operating-shadows-inside-nso-groups-corporate>; See also the recent revelations following the publication of the report by Citizen Lab already cited above, *Espionage against the European Parliament*, 3 July 2026.

exercising their Convention rights, or whether it was carried out under any legal framework capable of protecting against arbitrary interference.

14. The inherent logic of highly intrusive spyware therefore is that the rigorous safeguards developed by this Court to prevent abuse of technologically advanced surveillance regimes cannot be effective in this context. The Court in *Szabó and Vissy* was alive to this concern when it stated as follows -

*the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights ... it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives.*²⁸ (underlining added)

15. To be effective, the legal framework governing the use of spyware must therefore satisfy a standard of precision, foreseeability, and independent oversight that goes materially beyond what the Court has required for conventional surveillance. At a minimum, that framework must provide an explicit and specific legal basis for the acquisition and deployment of spyware, distinct from general provisions governing communication interception; require prior authorisation by a genuinely independent body with the technical capacity to assess the specific implications of spyware use; include additional safeguards calibrated to the particular risks spyware poses to professional secrecy categories, including journalistic source confidentiality; provide for mandatory notification to surveillance targets at the earliest point consistent with the operational purpose of the surveillance; and establish an independent audit mechanism capable of reviewing the full lifecycle of each use. In the absence of such provisions, the Intervener submits that a domestic legal framework cannot satisfy the requirement that any interference with Convention rights be “in accordance with the law” within the meaning of Articles 8 and 10.²⁹
16. The deployment of spyware against a journalist engaged in investigative reporting on matters of public interest is, in the ordinary case, unlikely to satisfy the necessity and proportionality requirements under those provisions. The indiscriminate access it provides, encompassing not only the journalist's own communications but also material that would expose the identities of sources, the scope of ongoing investigations, and legally privileged communications, means that even a legitimate investigative aim cannot justify the full extent of the intrusion. As the Court has held in the context of search and seizure of journalists' professional material, where an interference by its nature risks exposing source identities, the measure must be subject

²⁸ ECtHR, *Szabó and Vissy v. Hungary*, App. no. 37138/14, 12 January 2016, para 68.

²⁹ See ECtHR, *Green Alliance v Bulgaria*, App. no. 6580/22, paras 145 - 165, 17 February 2026.

to the most rigorous scrutiny regardless of the procedural safeguards nominally in place.³⁰

17. The indiscriminate and covert character of spyware described above produces consequences for press freedom that extend far beyond the individual journalist who is its immediate target.

Covert surveillance generates a severe chilling effect on investigative journalism

18. Restrictions on freedom of expression must be assessed having regard to the general context in which they operate, taking into account the deterrent effect they have on others who are not themselves directly targeted.³¹ Secret surveillance of journalists produces a chilling effect that operates at multiple levels and extends far beyond the individual journalist who is its immediate target. This Court has recognised that the chilling effect of measures restricting freedom of expression “works to the detriment of society as a whole”.³²
19. In the surveillance context, it acts as a deterrent from a particular line of investigation, causes sources to disengage for fear that their communications with the journalist are being monitored, and discourages other journalists, aware of the surveillance environment, from engaging in similarly sensitive reporting. The Council of Europe Commissioner for Human Rights has described the threat in the following terms: “Without constraints, surveillance becomes ubiquitous and increasingly intrusive, to the point that every actor is a potential target of surveillance and citizens curb their behaviour in that very knowledge.”³³
20. The combination of uncertainty as to whether the journalist has been placed under surveillance and the lack of available remedies is bound to create a profound chilling effect. This Court has emphasised the connection between the lack of availability of an effective remedy and the chilling effect, noting that -

*where the domestic system does not afford an effective remedy to the person who suspects that he was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the threat of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8.*³⁴

21. The chilling effect of covert surveillance does not depend on proof that any particular communication was intercepted or that any specific piece of information was obtained.

³⁰ ECtHR, *Nagla v. Latvia*, App. no. 73469/10, 16 July 2013, para 97; *Sorokin and Others v. Russia*, App. no. 73825/13, 27 June 2024, paras 61 – 63.

³¹ ECtHR, *Bladet Tromsø and Stensaas v. Norway* [GC], App. no. 21980/93, 20 May 1999, §64.

³² ECtHR, *Kaperzyński v. Poland*, App. no. 43206/07, 3 April 2012, §70.

³³ Council of Europe Commissioner for Human Rights, *Highly intrusive spyware threatens the essence of human rights* (January 2023), available at <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights>

³⁴ ECtHR, *Roman Zakharov v. Russia* [GC], App. no. 47143/06, 4 December 2015, §171.

The knowledge, or reasonable apprehension, that surveillance is taking place is itself sufficient to alter behaviour. For investigative journalists, who depend on relationships of trust with sources, this chilling effect is especially acute. The mere possibility of surveillance causes sources to withdraw and causes journalists to self-censor their methods of communication and the lines of investigation they pursue.

22. It follows that, in cases where a journalist claims to have been subjected to covert surveillance in connection with their investigative work, the assessment of whether there has been an interference with Article 8 and 10 rights cannot be limited to the question of whether specific acts of interception are proven. The creation of a surveillance environment in which investigative journalism is impeded, either through the targeting of a journalist or through the existence of a legal framework that permits such targeting without adequate safeguards, is itself an interference with the rights protected by those provisions that requires justification.
23. The chilling effect described above is compounded by the inherent characteristics of spyware that make it extremely difficult for those affected to establish, through domestic proceedings, that their rights have been violated.

Evidentiary difficulties in secret surveillance cases

24. The covert nature of surveillance creates evidentiary difficulties that are inherent to this category of case and cannot be resolved by the ordinary application of burden of proof rules. Although there may be variations in the factual circumstances, these difficulties arise from four interrelated features of the surveillance context: the absence of notification; the lack of domestic mechanisms enabling individuals to verify whether they have been subjected to surveillance; the challenges with respect to attribution given the secrecy surrounding states' acquisition and deployment of surveillance technologies; and the tendency of domestic courts to defer to state reliance on national security grounds.
25. The fact that forensic analysis of a device produces an inconclusive result cannot be taken to mean that the device was not infected. Spyware such as Pegasus is specifically designed to hide its traces and has been documented to manipulate system databases and records on infected devices in order to impede the research efforts of forensic investigators.³⁵ An inconclusive forensic result can still be consistent with infection and may in some cases be a product of the very technology whose presence is in issue. Where a state relies on the absence of conclusive forensic evidence as a basis for declining to investigate, it effectively uses the self-concealing design of the spyware as a shield against accountability.

³⁵See, for example, Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, 18 July 2021, available at <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

26. This Court has recognised that the covert nature of surveillance makes it inherently difficult for individuals to prove they were targeted.³⁶ In *Roman Zakharov v. Russia*, the Grand Chamber acknowledged the structural asymmetry between applicants and states in surveillance cases, and addressed this through a flexible approach to victim status that does not require proof of actual interception in all cases.³⁷ The Court held that where domestic law does not provide effective remedies, an applicant may claim to be a victim of a violation merely by reason of the existence of legislation permitting secret surveillance, if the relevant legislation is applied in practice to all users of telecommunications services.³⁸ The Intervener submits that this principle applies with particular force in cases involving journalists, given their heightened exposure to targeted surveillance and the especially serious consequences of such surveillance for the free flow of public interest information.
27. Secret surveillance occurs with exclusive knowledge of the authorities, making it impossible for targets to obtain evidence independently of those same authorities.³⁹ Where knowledge of events lies, by their nature, within the exclusive domain of the state, inferences of fact may arise and the burden of proof may shift accordingly. The Court has confirmed that inferences may be drawn from the respondent state's conduct in the proceedings before it, especially where the state alone has access to information capable of corroborating or refuting the applicant's allegations.⁴⁰ Where an applicant has provided a prima facie account of surveillance, including, for example, findings by independent digital security organisations of the kind that have been accepted in judicial proceedings in other jurisdictions, the burden rests on the respondent state to provide a satisfactory and convincing explanation.⁴¹ Journalists cannot reasonably be expected to furnish conclusive proof of covert, state-operated surveillance. To require them to do so would render the Convention's guarantees illusory in precisely the category of case where those guarantees are most needed.
28. The effectiveness of domestic remedies must also be assessed in light of these structural difficulties. A remedy that is theoretically available but practically inaccessible - because the evidence required to invoke it is held exclusively by the state, because national security exemptions are used to deny access to relevant files, or because oversight mechanisms lack genuine independence from the executive - does not satisfy the requirements of Article 13.⁴² The victim must seek redress from the authority that conducted the surveillance and must do so using evidence that authority controls and may invoke national security grounds to withhold.

³⁶ On evidential difficulties generally see, ECtHR, *Salman v. Turkey* [GC], App. no. 21986/93, 27 June 2000, para 100.

³⁷ *Roman Zakharov v. Russia* cited above paras 170 – 172.

³⁸ *Ibid.*, para 171.

³⁹ *Roman Zakharov v. Russia*, cited above, para 296; ECtHR, *Merabishvili v. Georgia* [GC], App. no. 72508/13, 28 November 2017, para 311.

⁴⁰ ECtHR, *Timutras v. Turkey*, App. no. 23531/94, 13 June 2000, para 66; ECtHR, *El-Masri v. the former Yugoslav Republic of Macedonia* [GC], App. no. 39630/09, 13 December 2012, para 152.

⁴¹ ECtHR, *Husayn (Abu Zubaydah) v. Poland*, App. no. 7511/13, 24 July 2014, para 396.

⁴² ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, App. nos. 72038/17 and 25237/18, 28 May 2024, paras 241–245.

29. Further, the Court has highlighted the importance of ensuring the individual under surveillance is notified of that fact by the state -

The question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned.”⁴³

30. In *Pietrzak and Bychawska-Siniarska* the Court noted that “a control mechanism for covert surveillance operations should preferably be based on an independent control body acting on its own initiative and possessing the legal instruments necessary to detect and combat abuses.”⁴⁴ But as noted above, the point of using spyware is precisely to evade detection and avoid scrutiny and accountability. In those circumstances, the only reasonable conclusion is that the deployment of highly invasive spyware cannot be reconciled with states’ obligations to provide an effective remedy.

Conclusion

31. This Court has repeatedly warned against the misuse of surveillance, recognising the severe implications this has for human rights and the rule of law.⁴⁵ It has highlighted the risks posed by unchecked surveillance powers and noted that surveillance can create a climate of fear that discourages those engaged in public interest reporting and legitimate political activity.⁴⁶ This case is therefore an opportunity for this Court to affirm clear standards for the protection of individuals’ Convention rights against covert surveillance operations involving spyware, and in particular to address the specific challenges that spyware poses to press freedom, source confidentiality, and the right to an effective remedy that the Intervener has sought to identify in these submissions.

Padraig Hughes

Media Defence

⁴³ ECtHR, *Szabó and Vissy v. Hungary*, App. no. 37138/14, 12 January 2016, para 86; ECtHR, *Roman Zakharov v Russia*, cited above, para 287.

⁴⁴ *Pietrzak and Bychawska-Siniarska and Others v. Poland*, cited above, para 195.

⁴⁵ ECtHR, *Big Brother Watch and Others v. United Kingdom*, App. nos. 58170/13, 62322/14 and 24960/15, para 332, in connection with Article 8 but also relevant to Article 10.

⁴⁶ ECtHR, *Green Alliance v Bulgaria*, App. no. 6580/22, para 148, 17 February 2026.

