European Court of Human Rights

***Nemanja POPOVIC against Austria,* Application No. 16530/23**

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL

Introduction and summary of intervention

1. This intervention is submitted by Privacy International (PI), pursuant to leave granted by the Vice-President of the Section on 17 October 2024 in accordance with Rule 44(3) of the Rules of Court. PI is a non-profit, non-governmental organisation (Charity Number: 1147471) that conducts research and advocates globally against government and corporate abuses of data and technology.

2. The present case concerns the interception of communications data by a non-Contracting State of the European Convention of Human Rights ("the Convention"), the cross-border sharing of the resultant information with a Contracting State, and its subsequent use in criminal proceedings.

3. This submission aims to contribute to the development of this Court's jurisprudence under Articles 8 and 6 of the Convention and will focus on the following:

    3.1. The impact of the interception of communications data on the right to privacy, including in the context of intelligence and law enforcement sharing;
    3.2. The privacy safeguards that should be implemented in the context of intelligence and law enforcement sharing;
    3.3. The impact on the right to fair trial through unlawful evidence arising from the failure to follow Article 8 safeguards; and
    3.4. The procedural and substantive safeguards necessary to prevent the violation of the right to a fair hearing where information to be admitted as evidence in criminal proceedings has been gathered in violation of the right to privacy.

i. The impact of the interception of communications data on the right to privacy including in the context of intelligence and law enforcement sharing

4. 'Communication and meta data' from an individual's phone reveal a great deal about them and the people with which they communicate. This Court has explained that "the patterns that will emerge" through meta data are "capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with".[1]

5. The collection of such communications data has accordingly been recognised by the Court of Justice of the European Union ("CJEU") as a "particularly serious" interference with privacy.[2] This Court has found that even "the mere retention and storage of personal data by public authorities is to be regarded as having a direct impact on the private-life interest of the individual concerned, irrespective of whether subsequent use is made of the data."[3]

6. Direct and unrestricted access to communications data is, therefore, akin to giving the police and intelligence agencies a master key (*passepartout*) to open the door to every house any time they

[1] *Big Brother Watch and Others v. The United Kingdom* (2021) App nos 58170/13, 62322/14 and 24960/15 (ECHR) §56 (see also §301) ("*Big Brother Watch ao*").
[2] *Privacy international v. Secretary of State for Foreign and Commonwealth Affairs* C-623/17, Judgment, 6 October 2020 §81.
[3] *Trajkovski and Chipovski v. North Macedonia* (2021) App Nos 53205/13 and 63320/13 (ECHR).

wish. Considering the intrusive nature of the interception of communications, it is subject to certain protections to guard against arbitrary or unlawful interference.[4]

7. The risk of arbitrary or unlawful interference is heightened when such a system operates in secret. This is particularly prevalent in the context of intelligence and law enforcement sharing. It often entails the interception and sharing of intelligence between multiple states – including between Contracting and non-Contracting States – which creates a complex and often opaque system which undermines human rights safeguards.

8. This context has been recognised by human rights bodies and experts, including the Office of the United Nations High Commissioner for Human Rights who noted:

> "Governments across the globe routinely share intelligence on individuals outside any legal framework and without adequate oversight. **Intelligence-sharing poses the serious risk that a State may use this approach to circumvent domestic legal constraints** by relying on others to obtain and then share information. Such a practice would fail the test of lawfulness and may undermine the essence of the right to privacy."[5]

9. We submit that this context poses a heightened risk and reiterate the assertion that "[w]hen the risk of State abuse increases, the Convention safeguards and corresponding domestic law guarantees should increase too."[6] These safeguards are discussed in more detail in the section below.

ii. The privacy safeguards that should be implemented in the context of intelligence and law enforcement sharing

10. There are multiple ways that intelligence and law enforcement agencies around the world collaborate and share information. It is typically done in one of three ways: 1) jointly, where two or more agencies or states agree to gather information together; 2) solicited, where an agency or state requests another body to gather or intercept communications on its behalf or 3) unsolicited, where an agency or state intercepts communications on its own initiative and shares it with another agency or state.

11. It is not always clear how an interception occurred, or even which countries or agencies were involved. As highlighted, intelligence sharing may occur outside any legal framework or in a relationship designed to circumvent domestic legal constraints. This poses a serious risk of interference with the right to privacy.

12. Article 8§2 requires *inter alia* that an interference with the right to privacy is in accordance with law, pursues one or more of the legitimate aims and is necessary in a democratic society to achieve such aims.[7] To be "in accordance with law" the impugned measure must have a basis in domestic law and be compatible with the rule of law.[8] This requires the law to be accessible and

---

[4] See for example *Big Brother Watch ao,* cited above; *Weber and Saravia v. Germany* (2006), Decision, App no 54934/00 (ECtHR) ("*Weber ao*"); *Roman Zakharov v. Russia* (2015) App. No. 47143/06 (ECHR) §230. ("*Roman Zakharov*"),

[5] Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc. A/HRC/39/29, 3 August 2018.

[6] *Big Brother Watch ao* cited above, §58 of the partly concurring and partly dissenting opinion of Judge Pinto De Albuquerque who was quoting *Szabó and Vissy v. Hungary* (2016) App No. 37138/14 §70 ("*Szabó ao")* with approval.

[7] See *Big Brother Watch ao,* cited above, §332; *Roman Zakharov* § 227; *Kennedy v. the United Kingdom* (2010) App. No. 26839/05 § 130.

[8] *Big Brother Watch ao,* cited above, §332.

for its effects to be foreseeable.[9] This Court has noted that "foreseeability" is different in the context of secret surveillance:

> "In the special context of secret measures of surveillance, such as the interception of communications, "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."[10]

13. To guard against the risk of arbitrary or unlawful secret surveillance, certain safeguards apply even where the information was obtained through intelligence sharing. These are discussed in more detail in the context of joint, solicited and unsolicited intelligence gathering.

The safeguards applicable to intercept material obtained during a joint investigation

14. In *Weber and Saravia v. Germany*, this Court set out minimum safeguards that must apply to any type of secret surveillance. Specifically any secret surveillance measure should respect "the following minimum safeguards that should be set out in statute law in order to avoid abuses of power": the nature of the offences; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of such measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[11]

15. These safeguards apply to the interception of communications in criminal investigations and where the interception was for reasons of national security.[12] In the context of national security, courts also consider "the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms, and the remedies provided for by national law."[13]

16. These safeguards accordingly apply to the interception of communications by a Contracting State when they undertake secret surveillance measures in concert with another state or agency, including non-Contracting States.

The safeguards applicable to solicited intercept material

17. This Court has recognised that in the context of solicited intercept material received from a non-Contracting state "the protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States."[14] Accordingly, the following safeguards apply:[15]

    17.1. Where a request is made to a non-contracting State for intercept material, the request must have a basis in domestic law;
    17.2. The law must be accessible to the person concerned and foreseeable as to its effects;
    17.3. There should be clear detailed rules that indicate the circumstances in which and the conditions on which the authorities are empowered to make such a request, and which

[9] See *Roman Zakharov,* cited above, §228.
[10] Ibid.
[11] *Weber ao,* cited above, § 95.
[12] *Big Brother Watch ao,* cited above, §335.
[13] Ibid.
[14] *Big Brother Watch ao,* cited above, §498.
[15] Ibid, §§497 – 499.

provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention; and

17.4. Upon receipt of the intercept material, the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction; and finally

17.5. Any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review.

18. We assert that these safeguards should be developed to include, at least, two additional safeguards concerning reasonable suspicion and notification. This is important in light of the risks posed by the opaque nature of intelligence sharing.

19. An authorisation to request intercept material should not focus only on the necessity and proportionality of a particular operation, but also on whether there is reasonable suspicion. In *Szabó*, the Court noted the requirement of "a sufficient factual basis for the application of secret intelligence gathering measures ... on the basis of an individual suspicion regarding the target person" as critical for "the authorising authority to perform an appropriate proportionality test".[16]

20. Similarly, 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."[17]

21. We submit that reasonable suspicion is a particularly important safeguard when material is shared concerning an individual for the purposes of criminal investigation. As we set out in further detail below, failure to verify reasonable suspicion at the point of judicial authorisation risks the selective presentation and potentially misleading inferences being drawn from evidence obtained by an investigation.

22. We submit that effective oversight cannot be limited to independent supervision and *ex post facto* review. The subjects of secret surveillance should always be notified (even if *post facto*). There is today an increasing consensus that notification requirements are necessary to enable individuals who are subjected to secret surveillance measures to challenge unlawful surveillance decisions.[18]

23. 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 remedy under Article 13.[19] 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

---

[16] *Szabó ao,* cited above, §71.
[17] *Roman Zakharov,* cited above, §260.
[18] A consideration of other countries' legislation shows that notification is both common and possible. See for example, Austria (Code of Criminal Procedure of the Republic of Austria 1975, Annex 2 (138)); Belgium (Belgium, Constitutional Court Case No. 145/2011 at paras 88 and 92); Canada (Canadian Criminal Code 1990, Part VI: Invasion of Privacy s 196(1)); Chile (Code of Criminal Procedure, Art 244); Estonia (The Security Authorities Act, Article 29); and Finland (Chapter 10, section 60 of the Finnish Coercive Measures Act).
[19] *Szabó ao,* cited above, §86. See also, *Association for European Integration and Human Rights*. *Association Ekimdzhiev v. Bulgaria*, (2007) App. No. 62540/001 (ECHR) §91.

measures taken without his or her knowledge and thus able to challenge their legality retrospectively".[20]

The safeguards applicable to the receipt of unsolicited intercept material

24. We submit that the receipt of unsolicited material from a foreign state by a Contracting State should be subject to appropriate safeguards. The protections afforded by the Convention would be circumvented and undermined if safeguards did not apply to unsolicited intercept material. Contracting States could simply enter into clandestine informal agreements with non-Contracting States for the receipt of unsolicited intelligence. Such a system cannot be Convention compliant.

25. The receipt and use of such material poses a heightened risk to the right to privacy. In light of its unsolicited nature, a receiving state is unlikely to know whether the material received was a product of unlawful interception, and it may not have been subjected to any safeguards concerning prior authorisation, reasonable suspicion or notification safeguards. There is accordingly a heightened risk of abuse in this context which requires increased corresponding safeguards.

26. In *Big Brother Watch ao,* this Court found that the safeguards it first developed in its case-law on the interception of communications by Contracting States applied equally to the receipt of *solicited* intercept material.[21] Specifically that upon receipt of the intercept material, "the receiving State must have in place adequate safeguards for its examination, use and storage, for its onward transmission; and for its erasure and destruction."[22] The Court acknowledged that this was particularly necessary in light of the fact that a receiving state may not always know whether the information it received was a product of interception.[23]

27. We submit that these safeguards apply equally in the context of unsolicited material received from a non-Contracting State. However, in light of the heightened risk posed, additional safeguards concerning judicial authorisation, reasonable suspicion, notification, and independent oversight should apply.

iii. Impact on the right to fair trial through unlawful evidence arising from the failure to follow Article 8 safeguards

28. In recent years, there has been a growth in the number of violations of Article 8 of the Convention during criminal investigations particularly in the context of the deployment of new surveillance technologies by law enforcement.[24] We note that this is likely to give rise to an increasing number of cases coming before this Court that raise issues relating to the interplay of potential unlawful evidence gathering in criminal investigations and the fairness of the subsequent proceedings pursuant to Article 6§1 of the Convention.

29. The deployment of surveillance technologies, such as the interception of communications data, to prepare, store, and manage evidence for use in criminal proceedings are characterised by opacity and asymmetry with regards to the information provided to the defence.[25]

---

[20] *Weber ao,* cited above, §135.
[21] *Big Brother Watch ao,* cited above, §498.
[22] Ibid.
[23] *Big Brother Watch ao,* cited above, §498.
[24] Radina Stoykova, "The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations", *Computer Law and Security Review,* volume 49, July 2023.
[25] PI, "Protest surveillance into courts: PI's report on the legal implications of unrestrained protest surveillance for the fair trial rights of activists, human rights defenders and protesters", November 2024, https://privacyinternational.org/report/5468/protest-surveillance-court

30. In this section of the Intervention, we address the impacts of breaches of Article 8 stemming from opaque surveillance measures in the evidence gathering phase on the right to fair trial under Article 6§1 of the Convention.

The interrelationship between national criminal procedures and Article 8 safeguards

31. A number of the recent cases that have come before the Court raising the issue of unlawful evidence gathering through surveillance and its impact on the right to fair trial are couched in terms of either breaches of Article 8 or national criminal procedure rules. This trend is highlighted by the recent Grand Chamber judgment in *Yüksel Yalçınkaya v. Türkiye* relating to a defendant's conviction on the sole basis of unlawfully obtained evidence regarding his use of the ByLock messaging service.

32. We note that the applicant raised submissions asserting that his Article 8 rights were breached due to the acquisition and use as evidence of information contrary to guarantees provided for under criminal procedure rules.[26] The Court declined to substantively consider the Article 8 claim on the basis that the applicant's submissions had concentrated on the fairness of using the evidence in criminal proceedings.[27] In doing so, it made a distinction between obtaining evidence in contravention of national rules of evidence and the interference with private life as a result of such unlawful action.[28]

33. The Intervener submits that the relationship between adherence to national criminal procedure rules regarding the collection and handing of evidence obtained through surveillance and safeguards necessary to comply with Article 8 of the Convention should nevertheless be considered closely linked in practice.

34. The close interrelationship between the safeguards under Article 8 and due process requirements under national criminal procedure was clearly articulated in the Joint Partly Concurring Opinions of Judges Pinto de Albuquerque and Bošnjak in *Dragoş Ioan Rusu v. Romania*.[29] As per §14 of this Intervention, the Article 8 safeguards relating to the interception of information through a joint investigation also contain a number of protections relating to the integrity of the information such as the need for procedures to examine, share, and delete information.

35. The Intervener submits that unlawful or arbitrary interference with one's personal information is an important aspect of Article 8 and failures to adhere to safeguards under the right to privacy may have downstream implications for the fairness of criminal proceedings. For this reason, there is an urgent need for a holistic approach that acknowledges the close interrelationship between due process safeguards contained in national criminal procedural rules and the right to privacy. The alternative risks a protection gap.

The negative impacts on fair trial arising from unlawful evidence gathering and sharing

36. As noted above at §17 above, unregulated intelligence sharing with non-Contracting States risks circumventing the protection afforded under the Convention. The Intervener submits that the risk of downstream fair trial impacts of intelligence that was shared in contravention of Article 8 of the Convention may similarly render protections under Article 6§1 "nugatory".

---

[26] ECtHR, *Yüksel Yalçınkaya v. Türkiye*, App. no. 15669/20, Judgment, 18 January 2023, §371.
[27] Ibid, §372.
[28] *Yüksel Yalçınkaya v. Türkiye,* cited above, §371.
[29] ECtHR, Joint Partly Concurring Opinions of Judges Pinto de Albuquerque and Bošnjak in *Dragoş Ioan Rusu v Romania, App.* no. 22767/08, Judgment, 31 October 2017, §10: where they asserted that conditions within criminal procedure rules regulating "*investigative acts that interfere with individual right…should correspond to the requirements of paragraph 2 of Article 8 of the Convention*".

37. For example, the right of notification under Article 8 of the Convention, which as stated above (§§22-23) must apply to covert surveillance, including with respect to information gathered and shared by a non-Contracting State, has a clear function in facilitating the exercise of fair trial rights.

38. In particular, we submit that non-notification is likely to limit the ability of the accused to prepare their defence and to ensure exculpatory electronic data is preserved.[30] The right to notification is not an absolute one, which must be balanced against legitimate interests of the state (including for example preventing harm to third parties, such as witnesses). Nevertheless, notification at the earliest possible interval could enable the lawfulness of information gathered to be tested before it is admitted into proceedings.

39. The presence of reasonable suspicion and the need to incorporate it within the prior judicial authorisation and review will also de-incentivise law enforcement from selectively presenting evidence in misleading ways to infer guilt. This is because surveillance without reasonable suspicion is more likely to result in everyday behaviours being recast as suspicious particularly where highly intrusive technologies are used that can amass significant information about an individual's private life.[31]

40. The nexus between the Article 8 safeguards, including prior independent judicial authorisation and oversight and the right to fair trial under Article 6§1 is exemplified by the Court's acknowledgement at §316 of *Yüksel Yalçınkaya* that:

> "Where the collection or processing of such information is not subject to prior independent authorisation or supervision, or a post factum judicial review, or where it is not accompanied by other procedural safeguards or corroborated by other evidence, its reliability may be more likely to be called into question."

41. The Intervener submits where the applicable Article 8 safeguards, including notification and judicial authorisation and oversight, are bypassed through intelligence sharing - this is likely to undermine the equality of arms and right to adversarial proceedings principles under Article 6§1 of the Convention.

42. Insofar as they concern the collection and use of evidence, these rights require that the parties have knowledge of and an equal opportunity to contest the arguments and evidence presented by the other.[32] We note that this in practice requires the disclosure of all materially relevant evidence to the accused.[33]

43. The lack of transparency and secrecy inherent in evidence gathering by law enforcement in contravention of the Article 8 safeguards addressed above makes it impossible for defendants to interrogate and challenge evidence from a position of parity. In particular, if the existence of the information is known – details of how it was gathered (including the technology used), how it was stored, with whom it was shared, and how it was used are unlikely to be available to the defendant.[34]

---

[30] Fair Trials, *The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters*, December 26, 2018 (Last updated: February 25, 2022), https://www.fairtrials.org/articles/publications/digital-or-not-fair-trial-principles-apply-challenges-of-e-evidence-and-the-right-to-a-fair-trial/.

[31] PI, *Protest surveillance into courts*, cited above.

[32] See for example, the Human Rights Committee, General Comment No.32 (CCPR/C/GC/32), §8, §13 and ECtHR, *Rowe and Davis v United Kingdom*, App. no. 28901/95, 16 February 2000, §60.

[33] *Rowe and Davis v United Kingdom,* cited above, §60.

[34] PI, *Protest surveillance into courts,* cited above.

44. We accept that divergences in procedural rights between the parties, including access to information, may be lawful where these distinctions are based in law, justified, and do not disadvantage the defendant.[35] However, it is not apparent to the Intervener that the conditions enabling lawful divergence in the level of disclosure can legitimately be met the context of unregulated evidence sharing. This is with reference to the importance of substantiating how evidence data was processed and the fact that a receiving Contracting State has no control over the conditions in which surveillance evidence was collected by the non-Contracting State particularly if it did not initiate the investigation.

45. We refer the Court to the preliminary reference of the Berlin Regional Court to the European Court of Justice (CJEU) regarding the use of evidence obtained through the hacking of EnchroChat data by French law enforcement agencies. The referring Court noted that in the context of narcotics trafficking offences (in which the material evidence predominantly relates to the negotiation of a narcotics sale):

> "…The defence depends not only on the analysis of individual messages, but also on the temporal and contextual connection between sent and received messages. Technical errors and incompleteness therefore entail a risk of chat histories being unintentionally distorted."[36]

46. What is important is not only the substance of communications, but also how and when the information was gathered. Such information is necessary to contextualise incriminating evidence and ensure that the defence is properly able to examine the integrity and accuracy of the evidence collected. The possibility to examine and test the modalities surrounding the evidence collection is particularly significant where the data obtained through surveillance is the sole information used to convict the accused.

iv. The necessary fair trial safeguards to ensure the fairness of the proceedings

47. As noted in the Partly Concurring Opinions of Judges Pinto de Albuquerque and Bošnjak in *Dragoş Ioan Rusu*, this Court's approach towards the question of when it is permissible under Article 6 to use evidence obtained in breach of any other Convention right is "far from settled".[37] In their Joint Opinion, they noted the importance of a number of criteria used to assess overall fairness in the context of evidence in breach of another Convention right.[38] In this section, we suggest necessary safeguards that we believe are required to ensure compliance with the overall fairness test under Article 6§1 of the Convention.

The proposed presumption of unfairness where information sharing contrary to Article 8 means that the evidence cannot be adequately challenged

48. The Intervener submits that that there should be a presumption that unlawful evidence obtained through information sharing with a non-Contracting state contrary to Article 8 will render the proceedings unfair for the purposes of Article 6§1. The presumption should apply where evidence was collected through surveillance without adherence to the Article 8 safeguards, we have

---

[35] PI, *Protest surveillance into courts,* cited above.
[36] CJEU, *Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice*, Case C-670/22, 24 October 2022.
[37] Joint Partly Concurring Opinions of Judges Pinto de Albuquerque and Bošnjak in *Dragoş Ioan Rusu v Romania,* cited above, §12.
[38] Joint Partly Concurring Opinions of Judges Pinto de Albuquerque and Bošnjak in *Dragoş Ioan Rusu v Romania* cited above, §§7-§11. We note the relevant criteria for assessing the overall fairness of proceedings in the context of evidence obtained in breach of another Convention right identified in the Opinion included *inter alia* the strength and reliability of the unlawful evidence, whether there is corroborating evidence, whether the defence was given the opportunity to challenge the authenticity of the evidence, and whether there are doubts as regards its accuracy or reliability (considering how it was obtained).

outlined above, such that it becomes impossible to interrogate the integrity, probity and accuracy of the relevant information the proceedings.

49. We submit that the Court's position in *Yüksel Yalçınkaya* represents a useful starting point when considering the need for the operation of the proposed presumption where a defendant cannot adequately challenge or interrogate evidence generated and shared in contravention of Article 8. We note that this Court stated in its judgments that its approach regarding electronic evidence did not mark a new departure from the overall fairness criteria.[39] Nevertheless, the Intervener submits that the Court's approach incorporates a fresh and welcome emphasis on the need for additional safeguards relating to the treatment of electronic evidence obtained through surveillance technology.[40] This shift moves away from a focus on the reliability and strength of unlawful evidence to one that underlines the conditions required for a defendant to be able to assess and challenge the reliability and integrity of electronic data in practice.

50. The conclusions reached by this Court also suggest that the overall fairness of the proceedings would be compromised where surveillance evidence cannot be adequately interrogated and challenged. Hence the need for a uniform presumption where these conditions cannot be met.

51. We submit that the proposed presumption would align with the approach articulated by the CJEU with respect to the implications of an EU Member State using evidence obtained and shared contrary to EU law. In its EnchroChat judgment, the CJEU found that where unlawful evidence was shared it would render the proceedings unfair to the extent that a party is not able to effectively comment on it.[41]

The proposed Article 6§1 safeguards in the context of unlawful evidence sharing contrary to Article 8 of the Convention

52. While as above, this Court did not substantively consider the applicant's Article 8 claim in *Yüksel Yalçınkaya above*; we consider that the necessary safeguards (hereinafter) that can be distilled from the judgment should also apply to evidence obtained and shared in breach of Article 8.

53. The necessary Article 6§1 safeguards should apply to evidence sharing contrary to the right to privacy, because of the interrelationship between Article 8 and criminal procedure safeguards and the fact that opaque cross-jurisdictional evidence sharing cannot incorporate the requisite level of transparency required for the accused to be able to interrogate incriminating information. This is for two reasons:

    53.1. The evidence gathering carried out by intelligence services or law enforcement, including in particular with respect to the interception of communications data, is itself characterised by high levels of opacity and secrecy. The secrecy regarding the methods pursued is likely to be a pre-condition for sharing the information in question. In this regard, we refer the Court to the CJEU's judgment in the EnchroChat case cited above[42]; and
    53.2. The receiving state will not be able to verify and therefore disclose to the defence how the evidence was obtained, stored, managed, and with whom it was shared. It will not be able to guarantee that material information was deleted or corrupted, including any exculpatory

[39] *Yüksel Yalçınkaya v. Türkiye,* cited above, §313.
[40] See for example, *Yüksel Yalçınkaya v. Türkiye,* cited above, §312: where the Court found that electronic evidence raises "*distinct reliability issues as it is inherently more prone to destruction, damage, alteration or manipulation*". See also §316 as referenced above at §11 of these submissions.
[41] CJEU, M.N., Case C-670/22, Judgment, 30 April 2024, §52: where CJEU noted that that the EnchroChat data requested by way of the European Investigation Order (EIO) could not be considered by an expert in the receiving EU Member State due to the 'defence secrets' classification conferred on them by the French authorities.
[42] *M.N.*, Case C-670/22, cited above, §130.

information. This is both for the reason of secrecy inherent in evidence gathering carried out by the state providing the information, but also because the receiving state will not have full access to the raw data, software and case management systems used in the investigation. The problem of insufficient access is likely to be heightened in the context of information sharing that is not initiated by the receiving state.

54. The Intervener submits that the necessary safeguards must be met in order to ensure that evidence can effectively be challenged and interrogated thereby ensuring that the presumption is not triggered. We believe that they should consist of the following.

55. Firstly, the defendant must be able to access the relevant raw data generated through the investigation.[43] This must include records of what surveillance technology was used, any investigative and forensic reports, and copies of chain of custody logs prepared by law enforcement confirming when the information was obtained, how it was stored, who had access to it, and with whom it was shared.[44] Where inferred data was gathered through a machine learning algorithm – copies of the input and training data should be provided to the defence.[45]

56. Secondly, the defence must be able to test and inspect the accuracy of data held as part of the investigation. This assessment should include the possibility for the appointment of independent experts to examine relevant technical evidence.[46] The defence should also be able to inspect a log of any evidence that was not shared with the receiving state in order to be able to ascertain if any exculpatory or otherwise relevant information is missing.

57. Thirdly, we consider that both these requirements should be subject to independent judicial oversight.

58. Finally, the Intervener submits that there is an urgent need for clarity as regards the interrelationship between the exclusion of unlawful evidence and the fairness of the proceedings pursuant to Article 6§1 of the Convention. We note that this Court has consistently held that the presence of an effective exclusionary remedy is unlikely to mean that the proceedings are unfair.[47] By the reverse logic, we submit that the absence of a clear exclusionary rule (or a failure to apply one) at the national level in the event that evidence gathered contrary to Article 8 would be impossible to effectively challenge or interrogate should as a matter of course trigger the proposed presumption.

59. Such a principle would ensure that the Court does not go beyond its remit in determining whether or not evidence is admissible and can be reconciled with the overall fairness test. Yet it would also recognise how depriving the defence of an opportunity to interrogate the integrity and accuracy of digital evidence vitiates the accused's effective participation in the proceedings. This is in line with the CJEU's approach taken in the EnchroChat case, which went even further and found that Member State courts should exclude evidence shared through an EIO in violation EU law in the event that the defendant is not in a position to comment effectively on the way it was collected.[48]

---

[43] *Yüksel Yalçınkaya v. Türkiye,* cited above, §331.
[44] PI*, Protest surveillance into courts,* cited above.
[45] PI*, Protest surveillance into courts,* cited above.
[46] *Yüksel Yalçınkaya v. Türkiye,* cited above, §333.
[47] See for example, ECtHR, *Ibrahim and others v the United Kingdom*, nos. 50541/08, 50571/08, 50573/08 and 40351/09, 13 September 2016, §274.
[48] *M.N.*, Case C-670/22 cited above, §131.

Conclusion

60. For the above reasons, the Intervener submits that the adherence to Article 8 safeguards in the context of transnational evidence sharing with non-Contracting States is of the utmost importance given the real risk that information sharing is used to circumvent the Convention. Due to the close relationship between Article 8 safeguards relating to law enforcement information sharing and national criminal procedure rules, this risk not only applies to the right to privacy but also the fairness of the proceedings as protected by Article 6 of the Convention. Failures to adhere to Article 8 safeguards when collecting and sharing electronic surveillance data, including in particular prior judicial authorisation and oversight as well as notification, may in turn compromise the equality of arms and the right to adversarial proceedings.

61. Hence there is a need for a holistic approach that considers both the Articles 6 and 8 implications of transnational evidence sharing. Where there is no means for a defendant to challenge and interrogate electronic evidence unlawfully obtained through surveillance or to exclude such information, the starting point must be that this would render the proceedings unfair for the purposes of Article 6§1. As we have demonstrated, a defendant will not be able to adequately challenge and interrogate surveillance evidence where he cannot comment on how it was processed. Both the Articles 8 and 6 safeguards we have advanced would facilitate legal certainty and de-incentivise the collection and sharing of evidence contrary to Article 8 by law enforcement as well as its further use in criminal proceedings.

Jonah Mendelsohn
Lawyer and Legal Officer
Privacy International

Tara Davis
Lawyer and Legal Officer
Privacy International