European Court of Human Rights

Bodinier and others v. France Application No. 40377/17

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 President of the Section in accordance with Rule 44(3) of the Rules of the Court. PI is a non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology.

2. The present case concerns the procedure created by French law No. 2015-912 for individuals to access and/or rectify data held in files concerning national security, defence, or public safety ("sovereign files"). This case presents an opportunity for the Court to address the safeguards available to individuals whose data is processed in the name of national security, defence, or public safety.

3. This submission aims to address (i) the issue of retention of data gathered as part as surveillance measures, (ii) the minimum necessary features of the national redress mechanisms, as well as (iii) supplement the standards set by this Court with the intervener's own experience of appearing as a complainant and litigating before the redress body of a Convention state.

(i) The retention of personal data gathered through surveillance measures amounts to an interference with Article 8 in its own right, and must be subject to safeguards

4. As a starting point, this Court has ruled that the mere storing of data relating to the private life of an individual amounts by the state to an interference within the meaning of Article 8, regardless of the subsequent use of that stored information.[1] It follows that the retention of data relating to private life constitutes an interference with the right to privacy.

5. In considering whether retention is proportionate and strikes a fair balance between the competing public and private interests, this Court has previously had regard to the length of any period of retention and its proportionality to the objective sought;[2] whether retention measures were differentiated or indiscriminate;[3] and avenues available to individuals to have any retained data removed.[4]

---

[1] ECtHR, *S. and Marper v. UK*, App. No. 30562/04, Judgment, 4 December 2008, paras. 67-68.
[2] ECtHR, *Aycaguer v. France*, App. No. 8806/12, Judgment, 22 June 2017, para. 42; *Gaughran v. UK*, App. No. 45245/15, Judgment, 12 February 2020, paras. 81-82.
[3] ECtHR, *S. and Marper v. UK* (n 1) paras. 119-120.
[4] Ibid., para. 119.

Length of retention

6. In assessing the length of retention, this Court has customarily applied a two-pronged approach, considering both any retention limits set out in law, as well as the practical significance and application of those limits.[5]

7. Where a regime does not set a definitive maximum time limit on the retention of data, the existence and functioning of certain safeguards enabling the deletion of that data becomes decisive.[6] Accordingly, a state allocating itself an unfettered power of indefinite retention can be regarded as having placed itself beyond the limit of the margin of appreciation.[7]

Indiscriminate retention measures

8. This Court has extensively considered the impact of blanket retention measures in the criminal justice context, finding that retention powers exercised in relation to DNA profiles, biometric data and photographs of offenders were in violation of Article 8 insofar as they did not take into account the nature and gravity of the offence.[8]

9. Similarly, the Court of Justice of European Union has repeatedly emphasised the prohibition of indiscriminate, blanket retention as part of measures combatting serious crime,[9] and has recently called for strict necessity and proportionality to apply, even in the context of national security measures.[10]

10. Indiscriminate surveillance measures should not be considered in isolation, and in the past this Court has found retention to be in violation of Article 8 where no real possibility of individual appeal existed.[11] More recently, this Court concluded that 'in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards"', including an appropriate redress mechanism.[12]

(ii) Minimum requirements apply to redress mechanisms available to subjects of surveillance

11. The assessment of whether the retention of data obtained as a result of surveillance measures is compliant with Article 8 is inextricably linked to the availability and quality of remedies that subjects of surveillance may avail themselves of. This Court has already highlighted certain minimum characteristics that a redress mechanism needs to present in cases of secret surveillance:

---

[5] ECtHR, *Aycaguer v. France* (n 2) para. 42.
[6] ECtHR, *Catt v. UK,* App. No. 43514/15, Judgment, 24 January 2019, para. 119.
[7] ECtHR, *Gaughran v. UK* (n 2) para. 88.
[8] ECtHR, *S. and Marper v. UK* (n 1) para. 119; *Gaughran v. UK* (n 2) para. 94.
[9] 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.103.
[10] CJEU, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Case C-623/17, Judgment, 6 October 2020, paras. 75-76.
[11] ECtHR, *Brunet v. France*, App. No. 21010/10, Judgment, 18 September 2014, paras. 41-42.
[12] ECtHR, *Big Brother Watch and others v. UK*, App. No. 58170/13, Judgment, 25 May 2021, para. 350.

i. First, it is recognised that the adequacy of any remedial procedure will be assessed in light of existing notification requirements.[13] Indeed 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".[14] It follows that the onus on the remedial procedure to safeguard rights is higher where there is no notification regime in place. Notably, this Court has highlighted that:

> *[…] in the absence of a notification requirement it is imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, in so far as possible, an adversarial process*.[15]

While this Court has not elaborated on the meaning of 'adversarial process' in the context of Article 8 safeguards, it has previously described it as one in which parties have an opportunity to have knowledge of and comment on all evidence adduced or observations filed with a view to influencing the court or other body's decision.[16]

ii. Second, the effectiveness of a remedy will depend on there being an adequate possibility of requesting and obtaining information about surveillance from the authorities. Accordingly, in *Zakharov,* the Court found that, while remedies were available in theory to subjects of surveillance, the absence of notification and the lack of an effective possibility of requesting and obtaining information about surveillance from the authorities meant that those remedies were not available in practice.[17]

iii. Third, the powers an authority possesses are relevant in determining whether a remedy is effective. This Court has found that, at a minimum, the decisions of a redress body "shall be reasoned and legally binding with regard to, among others, the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material".[18]

12. The above standards set clear expectations as to the characteristics that any remedial process available to subjects of surveillance must adopt in order to satisfy Article 8 safeguards. To supplement those standards, the intervener invites this Court to consider the comparative practice of an oversight authority in another Convention state, as well as the intervener's own experience in appearing before that authority in the context of surveillance challenges.

---

[13] ECtHR, *Big Brother Watch ao v. UK* (n 12) para. 337.
[14] ECtHR, *Weber and Saravia v. Germany*, App. No. 54934/00, Decision, 29 June 2006, para. 135.
[15] ECtHR, *Big Brother Watch ao v. UK* (n 12) para. 359.
[16] ECtHR, *Brandstetter v. Austria*, App. No. 11170/84, Judgment, 28 August 1991, para. 67.
[17] ECtHR, *Roman Zakharov v. Russia*, App. No. 47143/06, Judgment, 4 December 2015, paras. 291, 298.
[18] ECtHR, *Big Brother Watch ao v. UK* (n 12) para. 359.

(iii) Comparative experience of redress mechanisms suggests that it is both possible and necessary to achieve a better balance between interference with Article 8 and legitimate aims connected to national security

The United Kingdom's Investigatory Powers Tribunal

13. The Investigatory Powers Tribunal (IPT) is a specialised Tribunal established under the Regulation of Investigatory Powers Act 2000 to hear allegations by citizens of unlawful interference with their communications. The IPT has exclusive jurisdiction to investigate any complaint that a person's communications had been intercepted and, where interception has occurred, to examine the authority for such interception. This Court has in in the past examined the functioning and procedure of the IPT.[19]

14. The IPT is governed is by the Investigatory Powers Tribunal Rules 2018 (the IPT Rules), described by the IPT as containing

> *special provisions to cater for the fact that the secret nature of interception and surveillance operations and of security and intelligence gathering activities necessitate restrictions on the normal openness and adversarial nature of procedures for the adjudication of claims*.[20]

15. Accordingly, the IPT Rules impose restrictions:
    - on the disclosure of information contrary to the public interest or prejudicial to national security, the prevention of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services[21];
    - on the notification of determinations to the complainant if that determination is not in his favour[22]; and
    - allow for hearings to be held in private and excluding the complainant, i.e. 'in closed'.[23]

16. Despite the sensitive nature of the proceedings before the IPT, accommodations have been made to facilitate complainant participation. For example, in proceedings before the IPT, a complainant may attend hearings, make representations, give evidence and call witnesses.[24] Where the complainant's participation in proceedings before the IPT is restricted by virtue of their being unrepresented, disclosure of relevant documents to the complainant being objected to by the respondent, or a hearing held in the complainant's absence – all of which are restrictions foreseen under the Rules – the IPT may appoint Counsel to the Tribunal, who is empowered to make submissions in the complainant's interests.[25] Lastly, and only

[19] ECtHR, *Kennedy v. UK*, App. No. 26839/05, Judgment, 18 May 2010, paras. 75-98; ECtHR, *Big Brother Watch v. UK* (n 12) paras. 122-134;
[20] Investigatory Powers Tribunal, *C v. The Police*, IPT/03/32/H, Decision, 14 November 2006, para. 20.
[21] Rule 7(1), The Investigatory Powers Tribunal (IPT) Rules 2018.
[22] Rule 15(3), The IPT Rules 2018.
[23] Rule 10(2), The IPT Rules 2018.
[24] Rule 10(1), The IPT Rules 2018.
[25] Rule 12(1)-(2), The IPT Rules 2018.

when proceedings are decided in their favour, the complainant is entitled to an IPT determination, including any findings of fact.[26]

17. In an early ruling that preceded and substantially informed the 2018 Rules, the IPT considered its procedure in light of the standards imposed by Article 8 of the Convention. It asserted that:

    "[…] the impact of Article 8 on the Tribunal is that their procedure should provide adequate safeguards against the exercise of arbitrary power by the intelligence and security services and other public bodies equipped with investigatory powers, the exercise of which potentially interfere with the right to respect for private life and communications".[27]

    In that ruling, the IPT asserted that the procedural safeguards in respect of interference with Article 8 rights should be no less than those available under Article 6.[28] Assessing the procedure in force at the time, the IPT found that some of its rules fell short of necessary procedural safeguards.

18. Today, the IPT has a general duty, so far as possible, of openness, to conduct any hearing in public and in the presence of the complainant.[29] It has also powers to order disclosure, or if disclosure order is not complied with the order that admissions are made. [30]

19. It is noteworthy that the IPT extensively considered the "neither confirm nor deny" (NCND) domestic policy in that ruling. In brief, NCND is a statement of refusal to make a disclosure one way or the other on public interest grounds, which has since been judicially described not as a legal principle, but "a departure from procedural norms relating to pleading and disclosure".[31] All while recognising that the NCND policy was a legitimate objective, the IPT identified the task before it as an assessment of whether the Rules were strictly necessary and proportionate in achieving a reasonable relationship between interference with Convention rights and the objectives underlying the NCND policy.[32] The IPT's findings in relation to its own Rules – as outlined in the paragraph above – constituted an attempt by the Tribunal to move closer to what it considered to be the appropriate balance between the rights of the individual and legitimate objectives.

20. Currently, and as a matter of established practice, the IPT makes assumptions as to the significant facts of a case in favour of claimants and reaches conclusions on that basis; and it is only when it is concluded that the respondent's conduct would be unlawful on those assumptions, that the IPT will consider the position in a 'closed' session. In the IPT's own words: [33]

---

[26] Rule 15(2), The IPT Rules 2018.
[27] UK IPT, *Kennedy and Ors*, IPT/01/62 and IPT/0177, Ruling, 23 January 2003, para.112.
[28] Ibid., para.113.
[29] Rule 10(4), The IPT Rules 2018.
[30] Rule 7(7), The IPT Rules 2018.
[31] UK Court of Appeal, *Mohamed Ahmed Mohamed v. Secretary of State for the Home Department* [2014] EWCA Civ 559, para. 20.
[32] UK IPT, *Kennedy and Ors* (n 31) para.58.
[33] UK IPT, *Privacy International and Greennet & Ors v. Secretary of State for Foreign and Commonwealth Affairs*, IPT 14/85/CH and 14/120-126/CH, Judgment, 12 February 2016, para. 2.

> *"This procedure has enabled the Tribunal, on what is now a number of occasions, to hold open inter partes hearings, without possible damage to national security, while preserving, where appropriate, the Respondent's proper position of Neither Confirmed Nor Denied ("NCND").*

21. This Court first considered the role of the IPT in the context of Article 8 safeguards in *Kennedy*.[34] In that case, the Court found that the level of safeguards provided by the IPT was such that the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, insofar as any person who suspected that his communications were being or had been intercepted could apply to the IPT, and the IPT's jurisdiction did not depend on notification to the interception subject that there had been an interception.[35]

22. The IPT is only one example of a redress mechanism available to subjects of surveillance.[36] The experience of other states shows that, whatever its shortcomings, much more fair models are available. The Intervener invites the Court to establish a higher standard compatible with ECtHR jurisprudence.

Privacy International's experience appearing before the IPT

23. The Intervener has extensive experience undertaking IPT proceedings as a complainant. The Intervener has benefitted from the partially adversarial nature of the proceedings – on one occasion cross-examining a witness of the UK Government Communications Headquarters (GCHQ).[37] However, it has also experienced first-hand some of the shortcomings in the IPT's procedure, including: the lack of transparency; the 'closed' nature, length and complexity of proceedings; as well as limited access to relevant material, which is often either heavily redacted or simply unavailable to the complainant. These hurdles are such that it is only with great difficulty and resources that a complainant may pinpoint the occurrence and exact circumstances of any data misuse, eroding a complainant's ability to properly argue their case. In addition, the remedial proceedings once a violation of privacy has been identified fall short of an effective remedy. These are shortcomings that the Intervener strongly recommends other remedial mechanisms should avoid and invites the Court to set stronger safeguards to ensure the effective protection of the right to privacy.

24. The difficulties involved for complainants appearing before the IPT became apparent to the Intervener during its legal challenge to bulk personal datasets and bulk communications data regimes in the UK, where the Intervener argued that the UK intelligence agencies

[34] ECtHR, *Kennedy v. UK*, App. No. 26839/05, Judgment, 18 May 2010, paras. 167, 184-191.
[35] Ibid., para.167.
[36] s. 69, Regulation of Investigatory Powers Act 2000.
[37] UK IPT, *Privacy International v. The Secretary of State for Foreign and Commonwealth Affairs*, IPT/15/110/CH, Judgment, 23 July 2018, para.15.

practices were incompatible with ECHR and EU laws.[38] To that end, the intervener had to elicit significant evidence from UK's intelligence agencies' (namely MI5, MI6, and GCHQ) data collection and use practices. However, the information provided by the intelligence agencies was inconsistent in ways which were material, and therefore highly detrimental, to the legal proceedings. Two examples from these proceedings highlight our concerns.

25. In relation to the evidence provided by the GCHQ:

    i. GCHQ evidence originally alleged that it was the Foreign Secretary who made the decision as to which communications data was required to be provided by CSPs; an assertion that was later revealed, on GCHQ's own evidence, to be untrue.[39]
    ii. Similarly, aspects of GCHQ evidence remained unclear even after consecutive witness statements, including whether the Foreign Secretary's directions were made available to telecommunications providers, and whether it was specified to those telecommunications providers the data required by GCHQ.[40]

26. Overall, the number of mistakes and corrections needed in the respondent's evidence – both given in – 'open' and in 'closed'– was such that the IPT noted in its ruling that, in relation to the 'open' evidence, it was "regrettable that mistakes were made to begin with and not identified earlier" and, in relation to the 'closed' evidence – not seen by the Intervener – identified "five further serious such errors which had been picked up by the Respondents themselves and corrected".[41] As a result of the inconsistencies arising from the Respondents' evidence, the IPT reopened and revised its earlier judgment of October 2016, where it had concluded – as it later emerged, mistakenly – that the Foreign Secretary's directions were lawful.[42]

27. This instance is one of the few where the Intervener struggled with unreliable disclosures and it demonstrates the danger of relying heavily on 'closed' hearings in which claimants such as the Intervener cannot see, or challenge evidence presented by the government. It was only after sustained and tenacious questioning by the intervener in cross-examination – the first in the history of the IPT – that the government admitted errors in the sworn testimony it had previously submitted to the IPT.[43] Errors that the IPT in its initial revision of the provided material in open and closed did not identify.

28. Pursuant to the IPT Rules, the Intervener was simply not permitted to probe the evidence given in 'closed'. As the IPT itself recognises in its ruling, the serious errors affecting the 'closed' evidence were identified by the respondents themselves. As the Intervener had

[38] Privacy International, *Briefing on Legal Case: Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others*, July 2021. Available at: https://privacyinternational.org/long-read/4598/briefing-privacy-international-legal-case-bulk-personal-datasets-and-bulk
[39] UK IPT, *PI v. The Secretary of State for Foreign and Commonwealth Affairs* (n 43) paras. 12-16.
[40] Ibid., para. 36.
[41] UK IPT, *PI v. The Secretary of State for Foreign and Commonwealth Affairs* (n 43) para. 6 (iv).
[42] Ibid., para. 58. See earlier judgment: UK IPT, *Privacy International v. The Secretary of State for Foreign and Commonwealth Affairs*, IPT/15/110/CH, Judgment, 17 October 2016.
[43] Ibid., para. 15.

limited access to evidence, it is not possible to be certain that there were no other errors therein. Therefore, it is possible that further errors may have been discovered by the Intervener, had the opportunity to examine that material presented itself; or alternatively, that further probing by the Intervener would have resulted in further disclosure relevant to the case. Evidence provided by another agency indicate the shortfalls of this process.

29. The evidence provided by the UK Secret Service (MI5) during the proceedings have also proven subsequently to fall short of providing a complete account of the situation. On its 23 July 2018 decision the IPT decided that the acquisition and use of bulk personal datasets and bulk communications data were proportionate as required by Article 8 of the European Convention on Human Rights.[44] The IPT based its decision among others upon guarantees received by the intelligence agencies, including MI5, that appropriate safeguards were in place.

30. Later, MI5's disclosures in a separate legal challenge brought by a different complainant revealed longstanding and serious data management failings which affected the finding of fact in the intervener's earlier case, with an internal MI5 document dated January 2016 stating that "data might be being held in ungoverned spaces in contravention to our policies".[45] While this document and its contents had been available during and clearly relevant to the intervener's case, they were not disclosed in those proceedings. As a result, the Intervener, together with the other complainant Liberty, launched separate legal proceedings challenging these new findings and requested the reopening of the old claim, which are now pending.[46]

31. Where a complainant is prevented from accessing material relevant to their case, they are deprived from the opportunity to examine and challenge the quality of that evidence. The complainant must therefore trust the independent entity exercising review and supervision functions, as well as the very entities whose activity it seeks to challenge, to be meticulous and exacting. As the IPT examples shows, both actors are fallible. The lack of transparency; the 'closed' nature, length and complexity of proceedings; as well as limited access to relevant material, which is often either heavily redacted or simply unavailable reduce the accessibility and effectiveness of these proceedings.

32. As for access to remedy, the Intervener's experience in these proceedings were particularly concerning. In the course of those proceedings, a 'finding of fact' was made that all three agencies held data related to PI.[47] In addition, MI5 had accessed or examined the intervener's data. On the same day PI was informed that data had been deleted.[48] No further information or explanation was provided by either the intelligence agencies or the IPT as to what data had been processed, for what purpose, and under what conditions. The 'finding

[44] UK IPT, *PI v. The Secretary of State for Foreign and Commonwealth Affairs* (n 43) para.15.
[45] UK High Court of Justice, *R (Liberty) v. Secretary of State for the Home Department* [2019] EWHC 2057 (Admin), Judgment, 29 July 2019, para. 362.
[46] PI, MI5 ungoverned spaces challenge, available at https://privacyinternational.org/legal-action/mi5-ungoverned-spaces-challenge.
[47] UK IPT, *Privacy International v. The Secretary of State for Foreign and Commonwealth Affairs*, IPT/15/110/CH, Determination, 26 September 2018, para. 6.
[48] Ibid., para. 6.

of fact' was as such insufficient to allow the Intervener to satisfactorily exercise any data protection rights.

Relevance to the French legal framework

33. In surveillance cases, the key concern is whether the measures deployed are effectively unchallengeable and outside the supervision of the national judicial authorities and the Court.[49] A key aspect of a measure's "unchallengeability" is whether the relevant remedial procedure places an unrealistic and excessive burden on the complainant.[50] It is difficult to understand how a claimant without the Intervener's experience and without the support of the Intervener's counsel with established expertise in this area would have been able to benefit from this redress mechanism and succeed in their claim.

34. A further aspect for the Court to consider is the compatibility of onerous remedial procedures catering to data misuse complaints with data protection entitlements. Even in cases with a surveillance dimension, this Court's jurisprudence recognises the importance of preserving data protection entitlements when assessing an effective remedy, including access to one's personal data,[51] erasure,[52] and rectification.[53]

35. The intervener submits that, as a prerequisite for Article 8 safeguards to be met, the following requirements must be satisfied:

    i. The complaint should be heard before a body that while not necessarily judicial, is independent of the executive. The independence and impartiality of the redress mechanism should be assessed by the same standards that this Court has applied under the right to a fair trial. Independence prescribes independence from pressure. The rules establishing the appointments of the members of the panel should safeguard the process from any form of political influence.

    ii. The redress process should ensure the fairness of the proceedings. This Court's most recent position is that an adversarial process should unequivocally be followed where notification has *not* taken place.[54]
        a. There should be a presumption of an open hearing, where both parties are heard before the court. Only exceptionally the hearing should be heard in close without the complainant. In such cases, a special advocate should be appointed to represent the interests of the complainant that is able to directly consult with them in the process.
        b. Complainants should be able to examine all the material presented by the respondents in their case, regardless of whether they were notified of the

[49] ECtHR, *Roman Zakharov v. Russia* (n 17) para. 171; ECtHR, *Rotaru v. Romania*, App. No. 28341/95, Judgment, 4 May 2000, paras. 72-73.
[50] ECtHR, *Turek v. Slovakia*, App. No.57986/00, Judgment, 14 February 2006, para. 116.
[51] ECtHR, *Roman Zakharov v. Russia* (n 17) para. 291; ECtHR, *Segerstedt-Wiberg and others v. Sweden*, App. No. 62332/00, Judgment, 6 June 2006, para. 102.
[52] ECtHR, *Segerstedt-Wiberg and others v. Sweden* (n 51) para. 102.
[53] ECtHR, *Rotaru v. Romania* (n 49) para. 72.
[54] ECtHR, *Big Brother Watch ao v. UK* (n 12) para. 358.

surveillance measures deployed against them. This should include an opportunity for the complainant to cross-examine the respondent, as well as giving evidence and calling witnesses to make their case.

iii. In line with this Court's requirement for the decision of the redress body to be reasoned,[55] the complainant should be notified of the decision in their case regardless of the outcome, and at the very minimum be provided with complete findings of fact where they are successful. Such findings of fact should do more than merely confirm data misuse, and should describe, at a minimum, what data was processed; for what purpose; and for how long. Further, where data is erroneously held or simply inaccurate, the complainant should be in a position to request for that data to be erased or rectified. These safeguards are imperative to ensure the exercise of the right to an effective remedy.

20 September 2021

On behalf of the Intervener

Laura Lazaro Cabrera
Legal Officer
Privacy International
London EC1M 5UY

Ilia Siatitsa
Senior Legal Officer
Privacy International
London EC1M 5UY

[55] ECtHR, *Big Brother Watch ao v. UK* (n 12) para. 359.