DGI Directorate General of Human Rights and Rule of Law
Department for the Execution of Judgments of the ECtHR
F-67075 Strasbourg Cedex
FRANCE
Email: DGI-Execution@coe.int

10 March 2023

COMMUNICATION

In accordance with Rule 9.2. of the Rules of the Committee of Ministers regarding the supervision of the execution of judgments and of terms of friendly settlements:

Privacy International's Comments on the Action Plan submitted by the UK Government on 26 July 2022 to the Committee of Ministers, Council of Europe

Execution of judgment of the European Court of Human Rights
in *Catt v. the United Kingdom*
(App. no. 43514/15)

Background and introduction

In *Catt v. the United Kingdom* (App. no. 43514/15) [1], the European Court of Human Rights ("ECtHR") found a violation of the applicant's Article 8 Convention rights. In reaching this finding, the Court focused on two related issues. Firstly, the Court found that in this particular case there were compelling reasons for the ECtHR to assess the merits of the case, and that the UK's margin of appreciation did not preclude this assessment because the case concerned "personal data revealing political opinion which falls among the special categories of sensitive data attracting a heightened level of protection" (§112). Secondly, the Court found that there had not been a pressing need for the

[1] ECtHR, *Catt v. the United Kingdom*, Application No. 43514/15, Judgment, First Section, 24 January 2019, https://hudoc.echr.coe.int/eng?i=001-189424

police to retain Mr. Catt's data, and that therefore, its retention was disproportionate. In this regard, the Court held that, "in the absence of any rules setting a definitive maximum time limit on the retention of such data the applicant was entirely reliant on the diligent application of the highly flexible safeguards […] Where the state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive" (§ 119). The ECtHR also found that in this case, it was not clear "that [existing safeguards] were conducted in any meaningful way" (§121) and that even the safeguard allowing the applicant to request destruction of his data was of "limited impact given the refusal to delete his data" (§122). It is notable that the applicant in this case had no criminal record and was not considered a danger to anyone.

Privacy International (PI),[2] a non-governmental organisation based in London that works globally with partners, researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

PI has intervened as a third party in this Court previously in the cases, among others, of: *S. & Marper against the United Kingdom* (Application nos: 30562/04 and 30566/04), *Máté Szabó and Beatrix Vissy against Hungary* (Application no. 37138/14), *Khadija Ismayilova against Azerbaijan* (Application no. 65286/13), and *Mikolaj Pietrzak against Poland and Dominika BYCHAWSKA-SINIARSKA and others against Poland* (Applications nos. 72038/17 and 25237/18). Privacy International had also intervened on *Catt* case before this Court focussing on the surveillance emerging technologies deployed by the police (e.g. facial recognition, body warn camera, social media intelligence, etc.) and their effects on the right to privacy.[3]

PI has reviewed the Action Plan submitted by the UK Government in the *Catt v. UK* on 26 July 2022 and welcomes some of the general measures that the UK Government has completed in partial execution of the judgment of the ECtHR.[4] However, PI submits that the UK Government must still

[2] https://privacyinternational.org

[3] *Catt v. UK*, Third Party Intervention, Privacy International, 23 September 2016, https://privacyinternational.org/legal-action/catt-v-united-kingdom

[4] 1443rd meeting (September 2022) (DH) - Action plan (26/07/2022) - Communication from the United Kingdom concerning the case of *Catt v. the United Kingdom* (Application No. 43514/15) [DH-DD(2022)794] https://hudoc.exec.coe.int/ENG?i=004-52207

address significant gaps in its Action Plan in order to execute the judgment of the ECtHR. Below we expand on two of the key gaps we have identified.

Privacy International's comments regarding general measures

Firstly, and based on a review of the information shared about the general measures that have been pursued by the UK Government, a core issue arising out of the ECtHR's judgment in *Catt* v *UK* remains unaddressed, namely, ensuring that personal data, which is considered sensitive in accordance with the jurisprudence of the ECtHR and relevant legal frameworks, has "enhanced protection" within the relevant laws and guidance which protects people's Article 8 rights in the UK.

At present, the guidance which was updated as part of the UK Government's Action Plan[5] does not put in place specific procedural safeguards to ensure that sensitive personal data held by police forces must be specifically identified and/or reviewed to ensure that its retention remains lawful and necessary within the meaning of Article 8(2). The Authorised Professional Practice (APP) in relation to the management of police information (retention, review, and disposal), which was updated and referred to within the UK Government's Action Plan, makes general reference to the need for forces to give consideration "to the types of information that need to be retained, the length of that retention and the practical implications of storing these records in their various formats."[6] However, no reference is made to heightened review, retention, and disposal requirements for sensitive personal data, such as data revealing political opinions or religious beliefs, data revealing racial or ethnic origin, and other well-known categories of sensitive data.

Secondly, the creation of the National Common Intelligence Application (NCIA) database which replaces police forces' individual counter-terrorism databases must be subjected to robust, transparent, and effective safeguards in order to protect the right to privacy. A centralised policing database has the potential to capture, analyse, and retain unprecedented amounts of data about millions of people.

The UK government has stated in its Action Plan that, "a team of assessors [will] determine whether a record is relevant and necessary and whether it is proportionate for [a] record to be added to the

[5] See the College of Policing's Authorised Professional Practice "Review, retention and disposal" guidance, accessible online: https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal
[6] *Ibid.*

[NCIA] database…The work of the assessor team in the [Metropolitan Police Service] will be supported by a revised review, retention and disposal (RDD) policy in respect of the records held on the new NCIA database."[7] While PI welcomes the development of written RRD policy in respect of records held within this new database, it is still unclear whether or not the application of this policy will be subjected to oversight in order to check that they the safeguards in place are in fact being applied in a meaningful way. Based on a review of the information provided by the UK Government, there are no new mechanisms for accountability to ensure that the RRD policy is in fact being applied at all.

A recent judgment by the UK Investigatory Powers Tribunal (the IPT) - *Liberty and Privacy International v Security Service and Secretary of State for the Home Department* IPT/20/01/CH, exposed long-standing systemic breaches of RRD policies and legislative safeguards by the UK's internal intelligence agency – Security Service (or MI5). In that case, the IPT held that for years, MI5 acted unlawfully by knowingly handling people's personal data in systems that had "serious failings in compliance with review, retention and deletion policies" (§§66 and 79). Crucially, the IPT also held that despite MI5 knowing about issues with non-compliance at the most senior levels, the agency made a positive decision not to report its non-compliance to oversight bodies (§§82, 135, and 147). These failings amounted to a breach of Article 8 (§§138-139). Notably, the UK's Home Secretary was also found to have failed in its role as an oversight body (§107) in detecting and preventing the relevant compliance failings.

The findings by the UK Investigatory Powers Tribunal in the case brought against MI5 and the UK's Home Secretary are relevant to the execution of *Catt v. UK* because they highlight how without effective oversight and clear consequences for failures of implementation, the mere existence of RRD policies do not provide an effective safeguard for the right to privacy.

Conclusions and recommendations

At present and based on the information provided by the UK government in the Action Plan, we do not consider that the judgment in *Catt v. UK* has been executed. Most significantly, the ECtHR originally found that the policies in place led to the disproportionate retention of Mr. Catt's sensitive data, and that data which reveals political opinions requires enhanced protections. There remain significant gaps in the UK's policies which are intended to protect people's fundamental right to privacy by placing limits on police and law enforcement's information management systems.

[7] See page 3 of the UK Government's Action Plan.

In order to execute the judgment in *Catt v. UK*, this forthcoming policy must include specific procedural safeguards which relate to the disposal of sensitive personal data. As outlined in the judgment of the European Court, this type of data requires enhanced protection when it comes to reviews, retention, and disposal. Secondly, the creation of the National Common Intelligence Application (NCIA) database which replaces police forces' individual counter-terrorism databases must be subjected to robust, transparent, and effective safeguards in order to protect the right to privacy.

Nour Haidar
Legal Officer
Privacy International
Tel: +44 20 3422 4321
Email: nourh@privacyinternational.org

Dr. Ilia Siatitsa
Senior Legal Officer
Privacy International
Tel: +44 20 3422 4321
Email: ilia@privacyinternational.org