RIGHT TO PRIVACY

European Court of Human Rights, First Section, Catt v. United Kingdom, 24 january 2019.

The Court found that the UK violated the right to privacy (Article 8 of the European Convention on Human Rights) of Mr John Catt, a peace movement activist, who despite having never being convicted of any offence, had his name and other personal data included in a police database known as the "Extremism Database".

CASE OF CATT v. THE UNITED KINGDOM

(Application no. 43514/15)

JUDGMENT

STRASBOURG

24 January 2019

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Catt v. the United Kingdom,

The European Court of Human Rights (First Section), sitting as a Chamber composed of:

Linos-Alexandre Sicilianos, *President*,
Aleš Pejchal,
Ksenija Turković,
Armen Harutyunyan,
Pauliine Koskelo,
Tim Eicke,
Gilberto Felici, *judges*,
and Abel Campos, *Section Registrar*,

Having deliberated in private on 11 September 2018 and 11 December 2018,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in an application (no. 43514/15) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Mr John Oldroyd Catt, a British national, on 2 September 2015.

2. The applicant was represented by Mr S. Dutta of Bhatt Murphy Solicitors, a lawyer based in London. The United Kingdom Government ("the Government") were represented by their Agent, Ms R. Sagoo of the Foreign and Commonwealth Office.

3. On 19 May 2016 the application was communicated to the Government.

4. The Equality and Human Rights Commission and the NGO Privacy International were given leave to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 3 of the Rules of Court).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. The background facts

5. The applicant was born in 1925 and lives in Brighton.

6. The applicant has been active in the peace movement since 1948 and has been a regular attender at public demonstrations since then.

7. In 2005 the applicant began participating in demonstrations organised by Smash EDO. The object of Smash EDO was to close down the activities in the United Kingdom of EDO MBM Technology Ltd, a United States-owned company which manufactured weapons and weapon components and had a factory in Brighton. Serious disorder and criminality were features of a number of Smash EDO protests. Smash EDO protests therefore attracted a substantial policing presence.

8. The applicant was twice arrested at Smash EDO demonstrations for obstructing the public highway but has never been convicted of any offence.

9. In March 2010 the applicant made a subject access request to the police under section 7 of the Data Protection Act 1998 (see "Relevant domestic law and practice", below) for information relating to him. Sixty-six entries from nominal records for other individuals and information reports which incidentally mentioned him, concerning incidents between March 2005 and October 2009, were disclosed to him. Those records were held on a police database known as the "Extremism database", which at the relevant time was under the responsibility of the National Public Order Intelligence Unit of the police (NPOIU).

10. Most of the records related to demonstrations at the office of EDO MBM Technology Ltd but thirteen entries related to other demonstrations. They included, for example, the recording of his attendance at the Trades Union Congress ("TUC") Conference in Brighton in September 2006; at a demonstration at the Labour Party Conference in Bournemouth in September 2007; at a pro-Gaza demonstration in Brighton in January 2009 and at a demonstration against "New Labour" organised by a number of trade unions in September 2009. In the great majority of cases, the information recorded about Mr Catt was his name, presence, date of birth and address. In some cases his appearance was also described. A photograph of the applicant taken at a demonstration in September 2007 was also disclosed to him in response to his subject access request.

11. In August 2010 the applicant asked the Association of Chief Police Officers ("ACPO") to delete entries from nominal records and information reports which mentioned him. In September 2010 ACPO declined to do so. They did not give reasons.

12. On 17 November 2010 the applicant issued proceedings against ACPO for judicial review of the refusal to delete the data. He contended that the retention of his data was not "necessary" within the meaning of Article 8 § 2 of the Convention. Permission to seek judicial review was granted in March 2011 (see section B, below).

13. In January 2012, HM Inspectorate of Constabulary published a report on undercover police operations designed to obtain intelligence about protest movements (see paragraphs 50 to 53 below). The report concluded that information was being unnecessarily retained in police records. Although the report was concerned with covertly obtained intelligence, it also led to an extensive review of the database covering overtly obtained intelligence and

resulted in the deletion of a large number of nominal records and information reports. After that deletion process, the number of reports which mentioned the applicant was apparently reduced to two.

14. Following the judicial review proceedings, the applicant wrote to the police to make a further subject access request. The police replied on 12 November 2015 stating:

> "... the records are held to help UK policing manage a future risk of crime – of which [you] could be the victim. The records themselves should not and will not be disclosed [to you] for what are obvious reasons. An intelligence database loses all efficacy if it is not kept confidential."

15. In answer to a question asked by the Court when communicating the case the Government indicated that they had discovered four additional records mentioning the applicant in the database. They clarified that as a result, at the time the case was determined by the domestic courts there had in fact been six rather than two records in the database mentioning the applicant.

16. Of the four additional records, two concerned references to the domestic legal proceedings by third parties. The Government indicated in their submissions that one of those has since been deleted. The other two referred to the applicant. One was dated 15 April 2011 and detailed the applicant's presence at five separate events, not organised by Smash EDO, where there was a significant police operation and arrests occurred. The other was dated 19 July 2011 and related primarily to a third party but mentions the applicant's attendance at an event which was not organised by Smash EDO. There is no indication of whether there was any police presence or arrests at that event.

17. The Government stated that the police could not provide any explanation of why the reports were not disclosed previously. However, they were investigating the matter. They indicated that they had informed the Supreme Court and the applicant of the additional reports.

B. The domestic proceedings

1. Proceedings before the High Court

18. In a witness statement dated 6 June 2011 prepared in the context of the proceedings introduced by the applicant before the High Court, the then National Coordinator explained the functions of the National Public Order Intelligence Unit (NPOIU) and the position as regards retention of data relating to the applicant. In his witness statement, the National Coordinator clarified that the material which had been disclosed to the applicant following his subject access request of March 2010 was not all the material held in respect of the applicant: a considerable amount of further information had not been disclosed on the grounds that disclosure would prejudice the investigation or detection of crime and that the material was thus exempt from disclosure under section 29 of the Data Protection Act (see "Relevant domestic law and practice", below).

19. After explaining the nature of his activities and the various units supervised by him, the National Coordinator continued:

> "16. The term 'domestic extremism' is not prescribed by law. It is a descriptor generally used by the police service and partners to describe the activity of individuals or groups who carry out criminal acts of direct action to further their protest campaigns, outside the democratic process."

20. He then provided examples of how intelligence reports had assisted in policing a Smash EDO protest in 2010 and confirmed that, in his view, the applicant's data were being processed lawfully and fairly.

21. A hearing in the judicial review proceedings took place on 9 February 2012. With the agreement of the parties, the Commissioner of Police of the Metropolis was joined as a defendant. The High Court handed down its judgment on 30 May 2012. The court considered that Article 8 was not engaged in the case and that, even if it were, the interference was justified under Article 8 § 2. The applicant was granted permission to appeal by the Court of Appeal on 31 October 2012.

2. Proceedings before the Court of Appeal

22. Following a two day hearing during which legal representatives for the applicant, an NGO, the NHRI for England and Wales, ACPO and the Secretary of State presented their arguments, the Court of Appeal unanimously allowed the appeal in a judgment of 14 March 2014. It found that the inclusion of the applicant's personal data in the database constituted an interference with his Article 8 rights which was not justified. The court said that it did not doubt the importance to modern policing of detailed intelligence gathering and that it accepted the need for caution before overriding the judgment of the police about what information was likely to assist them in their task. It noted that, for present purposes, that task was to obtain a better understanding of how Smash EDO was organised in order to be able to forecast the place and nature of its next protest and to anticipate the number of people likely to attend and the tactics they were likely to adopt.

23. The court said that it was "not easy to understand how the information currently held on Mr Catt can provide any assistance in relation to any of those matters". It referred to the comment in the statement of the National Coordinator that it was valuable to have information about the applicant's attendance at protests because he associated with those who had a propensity to violence and crime. However, it considered that the statement did not explain why that was so, given that the applicant had been attending similar protests for many years without it being suggested that he had indulged in criminal activity or actively encouraged those that did. The court continued:

> "44. ... The systematic collection, processing and retention on a searchable database of personal information, even of a relatively routine kind, involves a significant interference with the right to respect for private life. It can be justified by showing that it serves the public interest in a sufficiently important way, but in this case the respondent has not in our view shown that the value of the information is sufficient to justify its continued

retention. It is striking that [the National Coordinator] does not say that the information held on Mr Catt over many years has in fact been of any assistance to the police at all. The Divisional Court considered that it was not practically possible to weed out from time to time information held on particular individuals. There is, however, no evidence to support this conclusion and we are not satisfied that it is correct. It should not be overlooked that the burden of proving that the interference with Mr Catt's article 8 rights is justified rests on the respondent.

45. That leaves the question whether the interference with Mr Catt's rights is in accordance with the law. This is very much a live issue given the relatively vague nature of some aspects of the regime contained in the MoPI Code and Guidance and the criticisms voiced by the Divisional Court in C (paragraph [54]) [see "Relevant domestic law and practice", below] and by the Strasbourg court in *M.M. v. the United Kingdom* (2012) (Application no. 24029/07). However, in the light of the conclusion to which we have come on the question of proportionality it is unnecessary for us to reach a final decision on the point."

3. Proceedings before the Supreme Court

24. The Supreme Court granted the Commissioner and ACPO leave to appeal. Following a three day hearing during which legal representatives for the applicant, an NGO, the NHRI for England and Wales, ACPO and the Secretary of State submitted arguments, it upheld the appeal in a judgment of 4 March 2015 by a majority of four justices to one. All five justices agreed that Article 8 was applicable and that retention of the data amounted to an interference with the applicant's rights under that article.

25. Lord Sumption delivered the leading opinion for the majority. He set out the applicable legal framework for collection and retention of data. After reviewing the requirements for "lawfulness" under Article 8 of the Convention, by reference to *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 99, ECHR 2008, he concluded that the interference was in accordance with the law. He noted that the Data Protection Act laid down principles that were germane and directly applicable to police information and contained a framework for their enforcement. These principles were supplemented by a statutory Code of Practice and administrative Guidance (see "Relevant domestic law and practice", below), compliance with which was mandatory. While, inevitably, there were discretionary elements in the scheme, their ambit was limited. Lord Sumption considered the applicant's argument that the Code of Practice and the Guidance did not enable him to know precisely what data would be obtained and stored or for how long to be unrealistic. He explained that the infinite variety of situations in which issues of compliance might arise and the inevitable element of judgment involved in assessing them made complete codification impossible. However, he noted, any person who thought that the police held personal information about him could seek access to it under section 7 of the Data Protection Act and, if he objected to its retention or use, could bring the matter before the Information Commissioner.

26. Lord Sumption then turned to consider the proportionality of the interference. He observed that political protest was a basic right recognised by the common law and protected by Articles 10 and 11 of the Convention. He

summarised the facts of the applicant's case, including the nature of Smash EDO's activities and the applicant's attendance at public demonstrations, and the framework for police collection and retention of data in this context. He concluded that the retention of information, including some which related to persons such as the applicant against whom no criminality was alleged, was justified. The starting point, in his view, was the nature and extent of the invasion of privacy involved in the retention of information of this kind, which he described as minor. While the information stored was personal information because it related to individuals, it was in no sense intimate or sensitive information. Rather, it was information about the overt activities in public places of individuals whose main object in attending the events in question was to draw public attention to their support for a cause. Although the collation of the information in the form in which it appeared in police records was not publicly available, the primary facts recorded were and always had been in the public domain; no intrusive procedures had been used to discover and record them.

27. He then addressed the justification for retaining the personal data for someone who has a clean record and for whom violent criminality must be a very remote prospect indeed. Referring back to the National Coordinator's statement (see paragraphs 18 to 20), he identified three reasons for the need to retain such data: (1) to enable the police to make a more informed assessment of the risks and threats to public order; (2) to investigate criminal offences where there have been any, and to identify potential witnesses and victims; (3) to study the leadership, organisation, tactics and methods of protest groups which have been persistently associated with violence. He also underlined some basic facts about intelligence-gathering commenting:

> "31 ... Most intelligence is necessarily acquired in the first instance indiscriminately. Its value can only be judged in hindsight, as subsequent analysis for particular purposes discloses a relevant pattern ... The most that can be done is to assess whether the value of the material is proportionate to the gravity of the threat to the public ..."

28. Lord Sumption further considered that the retention in a nominal record or information report of information about third persons such as the applicant did not carry any stigma of suspicion or guilt. It did not imply that all those mentioned as participating in events such as Smash EDO protests were being characterised as extremists. It was further noteworthy that the material was not usable or disclosable for any purpose other than police purposes, except as a result of an access request by the subject under the Data Protection Act. It was not used for political purposes or for any kind of victimisation of dissidents and was not available to potential employers. The material was also periodically reviewed for retention or deletion according to rational and proportionate criteria based on an assessment of danger to the public and value for policing purposes.

29. In conclusion, Lord Sumption was of the view that sufficient safeguards existed to ensure that personal information was not retained for longer than required for the purpose of maintaining public order and preventing or detecting crime, and that disclosure to third parties was properly restricted.

30. Lady Hale concurred with Lord Sumption but indicated:

> "51. ... it would be more objectionable if the police were to retain a nominal record collecting together all the information that they currently hold about him. Such dossiers require particular justification, not least because of their potentially chilling effect upon the right to engage in peaceful public protest. Mr Catt may be a regular attender at demonstrations, some of which are organised by a group which resorts to extreme tactics, but he himself has not been involved in criminal activity at those or any other demonstrations, nor is he likely to be in the future. Had the police kept a nominal record about him, therefore, I would have been inclined to agree with Lord Toulson that it could not be justified."

31. Lord Toulson, dissenting, agreed that the collection and retention of the data by the police was in accordance with the law. However, he considered that retention of the data was disproportionate. He explained that he had no difficulty in accepting in general terms the explanation given in the National Coordinator's statement, but that there had to be limits, particularly in the case of a person who had never been accused of violence and had been assessed not to be a threat. The statement did not explain why it was thought necessary to maintain for many years after the event information on someone whom the police had concluded, as they had in July 2010, was not known to have acted violently and did not appear to be involved in the coordination of the relevant events. Nor did it explain why it was thought necessary and proportionate to keep details of the applicant's attendance at other political protest events such as the Labour Party conference and the TUC conference.

32. He agreed with the Court of Appeal that the Commissioner had not shown that the value of the information relating to the applicant was sufficient to justify its continued retention. As to the suggestion that it would place too great a burden on the police to undertake frequent reviews, Lord Toulson pointed out that there was no evidence from the police that this would be over-burdensome. On the contrary, he said, the thrust of the evidence was that they did carry out regular reviews so there was nothing to indicate that deleting their historic records of the applicant's attendances at protest events would create any real burden.

33. Lord Toulson accepted that, when investigating serious organised crime, it was necessary for the police to be able to collate and keep records of the details of their investigations. However, he did not agree that there was any risk of that being hampered by upholding the decision of the Court of Appeal in the applicant's case. While the court should be slow to disagree with the evaluation of the potential usefulness of evidence by the police if a clear reason for it had been advanced, on the facts of this case Lord Toulson could not see what value they had identified by keeping indefinitely a record of the applicant's attendances at events where he had done no more than exercise his democratic right of peaceful protest. He concluded:

> "69. One might question why it really matters, if there is no risk of the police making inappropriate disclosure of the information to others. It matters because in modern society the state has very extensive powers of keeping records on its citizens. If a citizen's activities

are lawful, they should be free from the state keeping a record of them unless, and then only for as long as, such a record really needs to be kept in the public interest."

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. Power to collect and retain data

34. At common law the police have the power to obtain and store information for policing purposes including for the maintenance of public order and the prevention and detection of crime.

35. Under those powers the police have collected information relating to "domestic extremism" and this has resulted in the creation of the National Special Branch Intelligence System, commonly referred to as the "Extremism database". For the purposes of the domestic proceedings in the present case "domestic extremism" was defined as (see paragraph 18):

> "... the activity of individuals or groups who carry out criminal acts of direct action to further their protest campaigns, outside the democratic process."

36. In its June 2013 report reviewing the progress made against the recommendations in its 2012 report on the national police units which provide intelligence on criminality associated with protest, Her Majesty's Inspectorate of Constabulary identified three different working definitions of "domestic extremism" used by different bodies within the police (see paragraph 52, below).

B. The processing of personal data

1. The Data Protection Acts 1998 and 2018

37. The Data Protection Act 1998 regulated the processing of personal data. It required that the processing of data comply with the "data protection principles" in Schedule 1 to the Act. For a summary of the relevant principles see *M.M. v. the United Kingdom*, no. 24029/07, §§ 65-71, 13 November 2012. Part 2 of the Act was titled "Sensitive personal data":

> "In this Act "sensitive personal data" means personal data consisting of information as to—
>
> (a) the racial or ethnic origin of the data subject,
>
> (b) his political opinions,
>
> ...
>
> (d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),
>
> ..."

38. The Data Protection Act 1998 was repealed and replaced by the Data Protection Act 2018 which came into force on 27 May 2018. Chapter 2 of Part 3 of the Data Protection Act 2018 sets out the principles that apply to the

processing of data by law enforcement. Section 35 states that "sensitive processing" means the processing of personal data revealing "political opinions" or "trade union membership" *inter alia*. Section 42 provides for further safeguards in relation to such "sensitive processing".

39. Both the Data Protection Acts implement instruments of European Union Law all of which provided for "special categories" of personal data liable to higher protection than other types of personal data (see paragraphs 67-70 below).

2. Code of Practice on the Management of Police Information

40. Under section 39A of the Police Act 1996, the Secretary of State is empowered to issue codes of practice for the purpose of promoting the efficiency and effectiveness of police forces. A Code of Practice on the management of police information ("MoPI Code of Practice"), based on the provisions of the Data Protection Act, was issued by the Secretary of State in July 2005. Under the Code, handling of police information is limited to "police purposes". These are defined at paragraph 2.2 as protecting life and property, preserving order, preventing crime, bringing offenders to justice and performing any legal duty or responsibility of the police.

41. The MoPI Code of Practice provides for more detailed provision to be made by way of guidance. Such guidance (the "MoPI Guidance") was originally issued by ACPO in 2006 and updated by a new edition in 2010. It was later superseded by the Authorised Professional Practice: Information Management – Retention, review and disposal, published by the College of Policing in 2013. However, the 2013 Guidance appears substantially the same as the 2010 edition.

42. Section 2 of the 2010 MoPI Guidance addresses the processes for managing police information. It states at 2.2. that:

> "The management of records is fundamental to effective information management. The integrity of police information relies on the information being trusted, acceptable useable and available. To assist the evaluation, auctioning, sharing and review of information the information should be in a format that is accessible and easy to use, whether is an electronic, photographic or paper record."

43. Section 7 deals with the review of information for retention or disposal. It requires police information to be managed in compliance with the Convention, the Human Rights Act and the Data Protection Act. Paragraph 7.1 begins:

> "Reviewing information held by forces to determine its adequacy and continuing necessity for a policing purpose is a reliable means of meeting the requirements of the Data Protection Act. Review procedures should be practical, risk focused and able to identify information which is valuable to the policing purpose and needs to be retained. Review procedures should not be overly complex but should be as straightforward as is operationally possible."

44. Paragraph 7.2.1. states that the police force must act in a way that complies with the European Convention on Human Rights and the Human Rights Act 1998:

> "In relation to record retention this requires a proportionate approach to the personal information held about individuals. The decision to retain personal records should be proportionate to the person's risk of offending, and the risk of harm they pose to others and the community. A higher proportionality test should be met in order to retain records about relatively minor offending."

45. Paragraph 7.3.1 provides that the object of the review is to ensure that there is a continuing policing purpose for holding the record, that the record is adequate, up-to-date and not excessive, that the Data Protection Act is complied with, and that the assessment of the level of risk that the person presents is correct.

46. Paragraph 7.4 provides:

> "All records which are accurate, adequate, up to date and necessary for policing purposes will be held for a minimum of six years from the date of creation. This six-year minimum helps to ensure that forces have sufficient information to identify offending patterns over time, and helps guard against individuals' efforts to avoid detection for lengthy periods.
>
> Beyond the six-year period, there is a requirement to review whether it is still necessary to keep the record for a policing purpose. The review process specifies that forces may retain records only for as long as they are necessary."

47. A number of detailed criteria for carrying out this exercise are set out. Records are required to be subjected to an initial evaluation and then kept for a minimum of six years. Thereafter, they are subject to "triggered reviews", when information is added about the person in question; a statutory demand for access or disclosure is received; or a request for information is made by another law enforcement agency.

48. Appendix 4 to the guidance sets out scheduled reviews, which are fixed for information relating to individuals who have committed serious criminal offences or are considered dangerous to the public. The timing of these reviews varies with the nature of the information and the gravity of the risk. The Appendix specifies that records should be retained until persons reach 100 years old if they have been convicted or are suspected of involvement in offences involving the highest level of danger to the public. Otherwise, where retention limits are mentioned these refer to the minimum limits of 6 years retention or the length of sentence (if longer).

49. Paragraph 7.7 of the MoPI Guidance explains the need to collect and retain intelligence:

> "The retention of information relating to criminal activity and known and suspected offenders allows the Police Service to develop a more proactive approach to policing. By contributing to the identification of criminal patterns and threats and helping to prioritise the subsequent deployment of policing resources, information retention assists forces to prevent and detect crime and protect the public."

3. Oversight

50. Her Majesty's Inspectorate of Constabulary (HMIC) is a statutory organisation established under s.54 of the Police Act 1996 to inspect, and report to the Home Secretary and to Parliament on the efficiency and effectiveness of

the police forces in England and Wales. The HMIC has a remit to report on information management by the police.

51. Following revelations about the use of undercover policing in unrelated, domestic litigation HMIC announced they would review the systems used by the NPOIU to authorise and control the development of intelligence. HMIC published its "review of national police units which provide intelligence on criminality associated with protest" in 2012.

52. The report is focussed on reviewing the use of undercover policing. However, it does examine police work in this domain more widely including an analysis of "the NPOIU and its governance" in section 4 of the report, which also reviewed the work of its so-called sister units the National Extremism Tactical Co-ordination Unit and the National Domestic Extremism Team ("NDEU"). In this part of the report, it criticised the definition of "domestic extremism", stating:

> "This definition includes all forms of criminality, no matter how serious. It could lead to a wide range of protestors and protest groups being considered domestic extremists by the police. HMIC questions whether this is appropriate, and if the police should instead reserve this potentially emotive term for serious criminality."

53. The review also examined the intelligence systems used commenting:

> "... the NDEU is the sole national body for the collation and analysis of domestic extremism intelligence ... When intelligence is received by the NDEU it is recorded on a computer database ... During the early part of the 2000s, a weeding policy was developed which meant a record would be removed from the database if there had been no new intelligence for six months. However, this never formed a definitive policy; and in practice, by 2006 weeding was not robust. The current database has an automatic weeding process, although it still requires human confirmation. Since 2008 more than 2,900 expired entries and documents have been removed from the database.
>
> HMIC has examined the NDEU database and found that in a number of cases the rationale for recording and retaining the intelligence was not strong enough (in terms of the 'necessity and proportionately' tests). This makes it difficult for NDEU to provide assurance that these tests are satisfied. In order to meet the Management of Police Information requirements, NDEU must document 'objective facts' used to justify retaining intelligence. HMIC will revisit this issue separately."

54. In its July 2015 report "Building the Picture: An inspection of police information management" the HMIC stressing the importance of good information management stated in its national inspection findings:

> "It is a matter of serious concern that there is insufficient review taking place of the information that forces hold. Without these reviews – and the means to demonstrate that they have taken place properly or at all- the police service leaves itself vulnerable to challenge. The absence of sound and consistent reviews means that information might be destroyed when it should be kept, thus increasing the risk to public safety."

55. In its findings for the Metropolitan Police Service, which is the service that includes Special Branch, responsible for policing "domestic extremism", it commented:

> "The records management manual records how the force meets the retention, review and disposal elements of the APP [formerly the MOPI] guidance ... The length of time that

the force plans to keep information on systems was set out in the manual but the timescales were not consistent with either the previous MOPI or current APP standards. A review of the manual was planned during which the force approach will be matched to developing ICT [information communications technology]. All police information on force system was retained indefinitely. There was no process of review and no consistent process for deleting information once it is no longer useful. This situation increases risk of duplication and compromises investigation and analysis (see national recommendations 1 and 7)."

56. Recommendation 1 to chief constables was that they should ensure:

"... that a review is undertaken of the way in which their forces' information management policies and practice comply with the APP on information management so that they give effect to the national approach and minimise any divergence from that APP."

57. Recommendation 7 to the College of Policing was that it:

"... should amend its APP on information management so as to specify the minimum information management requirements for initial reviews in relation to the retention and disposal of information."

III. RELEVANT COUNCIL OF EUROPE INSTRUMENTS

Council of Europe

1. *The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (Treaty 108)*

58. Article 6 of the Convention titled "Special categories of data" states as follows:

"Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards ..."

59. In relation to Article 6 the Explanatory Report to the Convention comments:

"43. While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests. Categories of data which in all member States are considered to be especially sensitive are listed in this article."

60. The Convention was modernised, by means of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 10 October 2018 and Article 6 of the Convention, as amended by the Protocol, reads:

"1. The processing of:

- genetic data;

- personal data relating to offences, criminal proceedings and convictions, and related security measures;

- biometric data uniquely identifying a person;

- personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."

2. Committee of Ministers' Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector

61. Principle 3.a. states that the existence of electronic databanks in the public sector (defined as any electronic data processing system which is used to handle information) must have been provided for by law or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state.

62. Principle 4 states:

"Rules should be laid down to specify the time-limits beyond which certain categories of information may not be used or kept or used.

However, exceptions from this principle are acceptable if the use of the information for statistical, scientific or historical purposes requires its conservation for an indefinite duration. In that case, precautions should be taken to ensure that the privacy of the individuals concerned will not be prejudiced."

63. Principle 5 states:

"Every individual should have the right to know the information stored about him."

3. Committee of Ministers' Recommendation R (87) 15 to member states regulating the use of personal data in the police sector

64. The appendix to the recommendation sets out the basic principles in this context. Principle 2.1 – Collection of data, states:

"The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation."

65. Principle 2.4. states:

"The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry."

66. Principle 7 – length and storage of updating of data states:

"Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final

judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data."

IV. RELEVANT EUROPEAN UNION TEXTS

67. For a summary of relevant texts see *M.M. v. the United Kingdom*, cited above, §§ 143-148 and *Big Brother Watch and Others v. the United Kingdom* nos. 58170/13 and 2 others, §§ 217-220, *13 September 2018).*

68. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. It provided that the object of national laws on the processing of personal data is notably to protect the right to privacy as recognised both in Article 8 of the European Convention on Human Rights and in the general principles of Community law. Article 8 in the Directive prohibited the processing of special categories of data unless certain conditions were satisfied. The special categories of personal data identified were data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership ..."

69. With effect from April 2016 the 1995 Directive was replaced by the General Data Protection Regulation and Directive (EU) 2016/680 which sets out data protection principles in the context of law enforcement (the LED). Both of those instruments continue to impose special requirements concerning the processing of "special categories" of personal data. The LED defines 'processing' as:

> "... any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

70. Article 5 of the LED is titled "Time-limits for storage and review", it states:

> "Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed."

71. Article 10 of the LED provides:

> **"Processing of special categories of personal data**
>
> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:
>
> (a) where authorised by Union or Member State law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

72. The applicant complained that the retention of his data by the police was in violation of his right to privacy as provided in Article 8 of the Convention, which reads as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. Admissibility

73. The Government raised two arguments relating to admissibility.

74. The first was that the applicant was no longer a victim to the extent claimed in his application, because nearly all the entries in the database he complained of were deleted in 2012.

75. In this connection, the applicant underlined that his complaint was about the refusal of the police in 2010 to delete the sixty six records mentioning him in their database, which were collected and retained from 2004 onwards. The fact that all but six of those records were deleted in 2012 in the context of a weeding procedure triggered by revelations about undercover police work in unrelated domestic proceedings was not relevant.

76. The Court notes that the applicant's data was first collected and retained in 2005 (see paragraph 9, above). Since then, the police have continually retained his personal data on the database in one form or another. He has therefore had victim status from a Convention perspective since 2005. This conclusion is not affected by the fact that some of the applicant's personal data was deleted in 2012.

77. The second argument made by the Government was that the applicant had at his disposal a range of judicial remedies which he could have used to secure the deletion of his personal data.

78. The Court recalls that under its established case-law, when a remedy has been pursued, use of another remedy which has essentially the same objective is

not required (see, *inter alia*, *Micallef v. Malta* [GC], no. 17056/06, § 58, ECHR 2009 and *Kozacıoğlu v. Turkey* [GC], no. 2334/03, § 40, 19 February 2009).

79. In light of the above, the Court notes that the application is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

80. The applicant complained that the systematic collection and retention of information about him in a searchable database amounted to an interference with his right to privacy under Article 8. He argued that this interference was not justified because the database on which the data were held did not provide sufficient safeguards and so was not in accordance with the law. In particular he argued that the scope of the database may be adjusted arbitrarily by the police; data is retained for excessively long periods on the basis that the database as a whole may be useful; data is subject to automated and manual processing. He did not make arguments based on data protection legislation but submitted that the retention is unjustified given that the data retained related to his involvement in proper and lawful political protest activity and has never been useful for any police functions. The retention of such data is likely to have a chilling effect.

81. The applicant also argued that as records relating to him were found on the database after the Supreme Court's decision, the Supreme Court had made its decision on an incomplete factual basis. Recalling his assertion that the database had inadequate safeguards, the applicant argued that the fact records are not properly disclosed even in the context of proceedings before the Supreme Court indicates that the database is not in accordance with the law. He also alleged that there is no real system of oversight or independent review, emphasising that making a "subject access request" under the DPA will only be effective if all relevant data is disclosed by the police when they receive such a request. The applicant also asserted that the margin of appreciation to be afforded in light of the decisions of the domestic courts is reduced, given that those courts did not have all the relevant information before them.

82. The Government accepted that the collection and retention of information about the applicant constituted an interference with his right to respect for private life. However, relying on the findings of the Supreme Court, they contended that the interference was very limited.

83. They also relied on the findings of the Supreme Court that the interference was in accordance with the law, being subject to the Data Protection Act 1998, and a statutory Code of Practice and Guidance.

84. As to the necessity of storing the applicant's information, the Government underlined that the differences of view between the Court of Appeal and the Supreme Court reflect opinions properly open to both courts

on the evidence. With reference to the extensive amount of judicial scrutiny on this point at the domestic level, they contended that the question of whether it was necessary to retain the applicant's data falls within the state's margin of appreciation.

85. In relation to the disclosure of additional reports concerning the applicant after the domestic proceedings, the Government stated that these do not have any particular impact on the standing of the domestic judgments and that the applicant should make use of domestic remedies to bring a challenge concerning those disclosures, for example by way of judicial review.

2. The submissions of third party interveners

(a) The Equality and Human Rights Commission

86. The Equality and Human Rights Commission (EHRC) submitted remarks concerning the Extremism Database, which it characterised as a computerised and searchable police database which stores large quantities of intelligence about lawful public protests and those attending such protests. According to the EHRC, the database is not established under any legislation, has no statutory foundation, nor does any published policy refer to its creation, purposes or function.

87. The intervention recalls relevant standards and guidance set out in various international instruments including the Article 17 of the International Covenant on Civil and Political Rights and the Council of Europe's Committee of Ministers' Recommendation R(87) Regulating the use of personal data in the police sector. Drawing on the case law of this Court and the Court of Justice of the European Union, it goes on to set out what it considers to be the core minimum principles required to satisfy the requirement that a legal regime is "in accordance with the law" in the context of the police database at issue in this case. Those are:

(i) the creation of police powers must be published and accessible to the public;

(ii) clear and publicly accessible safeguards are required to ensure that the interference does not occur in an arbitrary, inappropriate or unnecessary manner;

(iii) there must be clear and accessible criteria enabling individuals, whose personal data is stored, to secure its deletion, including by way of independent review;

(iv) information relating to those not suspected of criminal activity must be removed.

88. The EHRC then concluded that the minimum safeguards are not present in relation to the Extremism Database. They also highlighted the danger of a chilling effect on legitimate political protests where the Extremism Database contains information about political activities.

(b) Privacy International

89. Privacy International is an NGO based in the United Kingdom and concerned with unlawful use of surveillance.

90. Privacy International criticised the Supreme Court's characterisation of the interference with the applicant's right to privacy as minor because it relates to activities that occurred in public, underlining that the collection of such information should be seen in its context. Privacy International argued that with rapid technological development, this approach would allow the monitoring of large amounts of information which is to some extent public, such as information from social media, facial recognition technology, body worn cameras, CCTV and automatic number plate recognition technology. It criticised the absence of legislation governing the collection and use of data obtained from such sources.

91. Privacy International concluded that the retention of such data is an infringement of privacy rights and also the right to freedom of expression, again underlining that such an infringement cannot be characterised as minor.

3. The Court's assessment

(a) Interference

92. In light of the conclusion of the Supreme Court, the Government conceded that the collection and retention of the applicant's personal data interfered with his Article 8 rights. However, they argued that the infringement in the applicant's rights was limited.

93. The Court recalls that it is well established in its case-law that the mere storing of information amounts to an interference with the applicants' right to respect for private life as secured by Article 8 § 1 of the Convention (see *S. and Marper*, cited above, § 67 and *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 73, ECHR 2006-VII with further references). The Court considers that the question of the alleged "limited" nature of the interference in the applicant's rights is more appropriately addressed in the context of whether the interference was necessary in a democratic society (see paragraphs 109-128, below).

(b) Justification

(i) In accordance with the law

94. As the Court has recalled the expression "in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope and discretion conferred on the competent authorities and the manner of its exercise (see, among other authorities, *M.M. v. the United Kingdom*, no. 24029/07, § 193, 13 November 2012 with further references).

95. The Court has also observed that there are various crucial stages at which data protection issues under Article 8 of the Convention may arise, including during collection, storage, use and communication of data (*M.M.,* cited above, § 195).

(a) Collection of data

96. Turning to the question of the collection of data, the Court notes that in the present case the collection of data was undertaken on the basis of general police powers in the common law, with reference to a working definition of "domestic extremism". That definition varied between bodies in the police, and its ambiguity has been criticised by HMIC (see paragraph 52 above).

97. In light of the general nature of the police powers and the variety of definitions of the term "domestic extremism", the Court considers that there was significant ambiguity over the criteria being used by the police to govern the collection of the data in question. It notes that perhaps as a result, the database in issue appears to have been assembled on a somewhat *ad hoc* basis. The Court therefore agrees with the applicant that from the information available it is difficult to determine the exact scope and content of the data being collected and compiled to form the database.

98. However, the Government have argued that the creation of the database does not need to be statutory. The Court considers that this assertion is supported by Principle 3.1. of the Committee of Ministers' Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (see paragraph 61 above) which states that such databanks must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state. In this connection the Court notes that the 'management' of data was regulated by legislation and a code of practice (see paragraphs 37-40 and paragraph 99) whilst the general police powers which permitted the collection of data were provided for in the common law. The Supreme Court referred to a HMIC report from 2003 (see § 28 of its judgment), and contemporaneous news reporting to support its conclusion that the collection of the applicant's data was foreseeable. The Court notes that the existence of a specific database was not clearly acknowledged until the domestic proceedings in this case, although it accepts that from the information publicly available it was possible to deduce that the police were likely to be maintaining such a database.

99. It is of concern that the collection of data for the purposes of the database did not have a clearer and more coherent legal base. However, the framework governing the collection of the applicant's data cannot be viewed in isolation from the provisions governing retention and use of the applicant's personal data. Accordingly, before coming to a conclusion under this head the Court turns to examine those provisions, which impose certain legal protections against arbitrariness.

(β) Retention and use of data

100. The Court has recently examined the provisions governing the retention of the data in the present case in *M.M.*, cited above. Those provisions were the Data Protection Act and the 2005 Code of Practice on the Management of Police Information. In the present case, those rules on retention of data stated that there was a presumption in favour of retention where data is not excessive, is necessary for a policing purpose, and is up to date. After the initial decision to retain, data must be retained for a minimum of six years. After that point it should be reviewed, and may be deleted. There is no fixed point in time identified for when reviews must take place, or when the data must be deleted. The police retain a general discretion to retain data if it is necessary to do so.

101. In *M.M.*, cited above, the Court found a violation of Article 8 on the basis that the retention and disclosure of personal data was not in accordance with the law. It observed that the indiscriminate and open-ended collection of criminal record data was unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, inter alia, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed. It also noted the absence of any mechanism for independent review of a decision to retain or disclose data (see *M.M.*, cited above, §§ 199- 206).

102. However, whilst the provisions on retention of data in this case bear some similarity to those in *M.M.*, other elements are not the same.

103. In the first instance, the Court notes that *M.M.* concerned the retention of criminal record data which the Court identified as not only personal but also sensitive, with "potentially devastating consequences" if disclosed. Moreover, the complaint in *M.M.* did not relate to police intelligence gathering but focussed on the disclosure regime for criminal records, and the Court criticised the absence of a statutory framework governing the (in some cases obligatory) communication of such data by the police to prospective employers in Northern Ireland at the time (see *M.M.*, cited above, § 203).

104. Against this background, the Court also notes that in contrast to the applicant in *M.M.,* the applicant in the present case had the possibility to make a request for the review and deletion of his data which he exercised (see *a contrario M.M.,* cited above*,* § 206*).*

(γ) Conclusion

105. The Court has concerns about the ambiguity of the legal basis for the collection of the applicant's personal data. In particular the Court notes the loosely defined notion of "domestic extremism" and the fact that applicant's data could potentially be retained indefinitely. However, the data retained would not be disclosed to third parties; and the applicant had the possibility to apply for the deletion of his data.

106. In this connection, the Court recalls that the question of whether the collection, retention and use of the applicant's personal data was in accordance

with the law is closely related to the broader issue of whether the interference was necessary in a democratic society (*S. and Marper,* cited above, § 99, ECHR 2008).

107. Therefore, in view of its analysis in paragraphs 109-128 below, the Court does not find it necessary to decide whether the interference was "in accordance with the law", within the meaning of Article 8 § 2 of the Convention.

(ii) Legitimate aim

108. There has been no significant dispute about whether the creation and maintenance of the database by the police pursues a legitimate aim. The Court equally considers that it does so, that aim being the prevention of disorder or crime and safeguarding the rights and freedoms of others.

(iii) Necessary in a democratic society.

109. The Court has set out on many occasions the elements to be taken into account when considering whether an interference in an applicant's Article 8 rights was necessary and therefore justified. It will be necessary in a democratic society if it answers to a "pressing social need", if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient". A margin of appreciation must be left to the competent national authorities in this assessment (see *S. and Marper,* cited above, § 101-102).

110. Dealing with the latter element first, the Court notes the Government argued that the domestic courts had closely examined the issues in light of Article 8. Those courts differed in their conclusions but this indicated that the point was one upon which a correct application of the principles under Article 8 could nonetheless result in a different result. With reference to the extensive amount of judicial scrutiny at the domestic level, they contended that the question of whether it was necessary to retain the applicant's data falls within the state's margin of appreciation and it was therefore not for this Court to decide.

111. In this respect, the Court recalls that in Article 8 cases it has generally understood the margin of appreciation to mean that, where the independent and impartial domestic courts have carefully examined the facts, applying the relevant human rights standards consistently with the Convention and its case-law, and adequately balanced the applicant's personal interests against the more general public interest in the case, it is not for it to substitute its own assessment of the merits (including, in particular, its own assessment of the factual details of proportionality) for that of the competent national authorities, unless there are shown to be compelling reasons for doing so (see *McDonald v. the United Kingdom*, no. 4241/12, § 57, 20 May 2014).

112. However, the Court considers in the present case there are reasons for doing so. In the first place it considers significant that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 58-60 and 67-70 above and *S. and*

Marper, cited above, § 76). It notes that at the domestic level this element of the complaint was characterised as one of data protection law and was not a particular focus of the litigation. Having concluded that retention of the applicant's data was not justified under Article 8, the Court of Appeal did not consider that examining the specific principles of data protection would add anything to their analysis (see § 65). The applicant did not pursue specific data protection arguments before the Supreme Court, which therefore only referred to data protection law generally in the context of lawfulness. However, the Court considers that the nature of the applicant's complaint meant that the sensitive nature of the data in question was a central feature of the case both before the domestic courts as well as before this Court (see paragraph 80 above).

113. The Court also notes that notwithstanding its well established case-law (see paragraph 93, above) the High Court considered that the collection and retention of the applicant's data was not an interference under Article 8. This question was resolved by the Court of Appeal and Supreme Court who found that it was an interference and gave detailed and comprehensive judgments referring extensively to Strasbourg jurisprudence. However the Government maintained arguments that the retention was not systematic and the nature of the interference was limited. The applicant argued that a decisive ruling was necessary. The Court agrees that some clarification of these elements appears to be called for.

114. The Court also recalls the importance of examining compliance with the principles of Article 8 where the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 229, ECHR 2015, and *Szabó and Vissy v. Hungary*, no. 37138/14, § 68, 12 January 2016). Unlike the present case, those cases dealt with covert surveillance. However, the Court considers it should be guided by this approach especially where it has already highlighted concerns relating to the ambiguity of the state's powers in this domain (see paragraph 105 above).

115. Finally, the Court takes into account the manner and timing of the disclosure and the fact that there was more personal data held on the applicant than revealed at the time of the domestic proceedings (see paragraphs 11, 15-17 above). This has an impact on its evaluation of the available safeguards (see paragraph 122 below).

116. Therefore, the Court turns to the other elements to be examined, beginning with the question of whether there was a "pressing social need" to collect and retain the applicant's personal data. In doing so, it recalls that the question for it to examine is not whether there was a "pressing social need" for the police to establish and maintain such a database. To the extent that the Court examines this issue from a more general aspect, it has done so in its conclusion that the creation of the database pursued a legitimate aim (see paragraph 108 above). At this stage, the Court is examining whether the collection and retention of the applicant's personal data may be regarded as justified under the Convention (see *mutatis mutandis, S. and Marper,* cited above, § 106).

117. As to whether there was a pressing need to collect the personal data about the applicant, the Court accepts that there was. It agrees with the Supreme Court that it is in the nature of intelligence gathering that the police will first need to collect the data, before evaluating its value (see paragraph 27, above). In this respect, the Court again recalls that the personal data in question was overtly obtained.

118. The Court also agrees with the domestic courts that the police had an obvious role to monitor protests of Smash EDO where the activities of that group were known to be violent and potentially criminal. Therefore, even if the applicant himself was not suspected of being directly involved in that group's criminal activities, it was justifiable for the police to collect his personal data. He had after all decided to repeatedly and publicly align himself with the activities of a violent protest group.

119. As to whether there was a pressing need to retain the applicant's data, the Court considers there was not. It shares the domestic courts' concern that there is a need for caution before overriding the judgment of the police about what information is likely to assist them in their task (see paragraph 22 above). In this respect, the Court underlines that its conclusion does not call into question the fact that there may have been a pressing need for the police to retain the applicant's personal data for a period of time after it was collected. However, 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 in the MOPI to ensure the proportionate retention of his data. Where the state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive (see *mutatis mutandis S.M.M. v. the United Kingdom*, no. 77450/12, § 84, 22 June 2017). Those safeguards must enable the deletion of any such data, once its continued retention becomes disproportionate.

120. In this connection, the Court observes that as the applicant's personal data could potentially be retained indefinitely the only time limit that he could be certain of was that the data would held for a minimum of six years, at which point it would be subject to a scheduled review. In the present case, it is not clear that these six year reviews or any later reviews were conducted in any meaningful way. Certainly, they did not directly result in the deletion of any of the applicant's personal data.

121. The Court notes that the circumstances of the case contrast with the approach set out in principle 4 of the Committee of Ministers' Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis the electronic data banks in the public sector, which states that rules should be laid down to specify maximum time-limits beyond which certain categories of information may not be used or kept, other than in some exceptional situations (see paragraph 62 above).

122. Also, whilst the applicant could and did request the disclosure and destruction of his data, this safeguard appears to have been of limited impact given the refusal to delete his data or to provide any explanation for its continued

retention – including the later disclosure without explanation of the retention of additional data (see paragraphs 11 and 15-17 above). So far as the Court is aware, at least some of the applicant's personal data concerning his involvement in non-violent protest was collected over six years ago and remains in the domestic extremism database (see paragraph 16, above) despite the fact that the police concluded, and the domestic courts affirmed that the applicant was not considered a danger to anyone (see paragraph 31, above).

123. Moreover, the absence of effective safeguards was of particular concern in the present case, as personal data revealing political opinions attracts a heightened level of protection (see paragraph 112 above). Engaging in peaceful protest has specific protection under Article 11 of the Convention, which also contains special protection for trade unions, whose events the applicant attended (see paragraph 10, above). In this connection it notes that in the National Coordinator's statement, the definition of "domestic extremism" refers to collection of data on groups and individuals who act "outside the democratic process". Therefore, the police do not appear to have respected their own definition (fluid as it may have been (see paragraph 105)) in retaining data on the applicant's association with peaceful, political events: such events are a vital part of the democratic process (see *Gorzelik and Others v. Poland* [GC], no. 44158/98, § 92, ECHR 2004-I). The Court has already highlighted the danger of an ambiguous approach to the scope of data collection in the present case (see paragraph 97 above). Accordingly, it considers that the decisions to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a "chilling effect".

124. Moreover, principle 2 on the collection of data in Recommendation R (87) 15 (see paragraph 65 above) states that the collection of data on individuals solely on the basis that they belong to particular movements or organisations which are not proscribed by law should be prohibited unless absolutely necessary or for the purposes of a particular inquiry (see mutatis mutandis *Segerstedt-Wiberg and Others,* cited above, § 79). The Court considers that the retention of the applicant's data in particular concerning peaceful protest has neither been shown to be absolutely necessary, nor for the purposes of a particular inquiry.

125. The Court also underlines that it makes these findings about the applicant in light also of his age, which Principle 7 of Recommendation R (87) 15 identifies as a particular consideration in this context (see paragraph 66 above).

126. The Government have argued that it would be too burdensome to review the database and delete all the entries relating to the applicant, because the database is not fully automated. However, the Court notes that the MoPI guidance provides for the data to be reviewed after six years and deleted. Whilst this does not appear to have happened in the present case it nonetheless shows that review and deletion of records was intended to be a real possibility. In this connection the Court also recalls that in 2012 following the HMIC report, a

significant number of personal data records were deleted, clearly indicating that review and deletion of records is possible (see paragraph 13, above). The Court also notes the MoPI guidance stipulates the importance of ensuring that information is easy to access and use (see paragraph 42, above).

127. Accordingly, the Court is not convinced that deletion of the data would be so burdensome as to render it unreasonable. In general terms the Court would add that it would be entirely contrary to the need to protect private life under Article 8 if the Government could create a database in such a manner that the data in it could not be easily reviewed or edited, and then use this development as a justification to refuse to remove information from that database.

128. The foregoing considerations are sufficient to enable the Court to conclude that there has been a violation of Article 8 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

129. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

130. The applicant did not submit a claim for just satisfaction, considering that a finding of a violation would be sufficient. Accordingly, the Court considers that there is no call to award him any sum on that account.

B. Costs and expenses

131. The applicant also claimed GBP 41,770 for the costs and expenses incurred before the Court and attached detailed documentation in support of their claim.

132. The Government claimed that this figure was excessive, in particular as the lawyers' hourly rates were too high and their pleadings repeated arguments made before the domestic courts.

133. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 27,000 for the proceedings before the Court.

C. Default interest

134. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
      (i) EUR 27,000 (Twenty-seven thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 24 January 2019, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Abel Campos Registrar	Linos-Alexandre Sicilianos President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Koskelo, joined by Judge Felici, is annexed to this judgment.

L.-A.S
A.C.

CONCURRING OPINION OF JUDGE KOSKELO JOINED BY JUDGE FELICI

A. Approach to the case

1. I agree with the outcome of this case, namely that there has been a violation of the applicant's rights under Article 8 of the Convention. The majority in the Chamber have reached this conclusion following an analysis as to whether the impugned interference was "necessary" within the meaning of Article 8 § 2 of the Convention. I do not have any major objections to the essence of that analysis as such. The misgivings I have are in relation to the preceding analysis of whether the interference with the applicant's rights under Article 8 was "in accordance with the law". On this point, the majority do identify a number of concerns but consider that it is not necessary in the present case to reach any firm conclusion as to whether the requirement of lawfulness has been met. Regrettably, I find the approach adopted in this respect lacking in firmness as well as in consistency with existing case-law.

2. According to the Court's well-established case-law, the phrase "in accordance with the law" in Article 8 § 2 of the Convention requires not only that the impugned measure must have a basis in domestic law but that it must also be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and is inherent in the object and purpose of Article 8. Thus, the requirement of lawfulness also refers to the quality of the law in question. This entails that the law should be adequately accessible and foreseeable as to its effects, that is to say formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct (see, for instance, *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 95, ECHR 2008).

3. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and, accordingly, indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. The level of precision required of the domestic law – which cannot provide for every eventuality – depends to a considerable degree on the context and content of the law in question, such as the field it is designed to cover (ibid. § 96).

4. In the field of data protection, the Court has considered it essential for the applicable law to provide clear, detailed rules governing the scope and application of the relevant measures as well as sufficient guarantees against the risk of abuse and arbitrariness at each stage of the processing of personal data (see *M.M. v. the United Kingdom*, no. 24029/07, § 195, 13 November 2012, and *Surikov v. Ukraine*, no. 42788/06, § 74, 26 January 2017; both with further references). These are indeed crucial requirements.

5. In a context such as the present one, namely the processing by the police of personal data, including sensitive data, for the purposes of managing threats to public order, particular vigilance is called for when assessing the requirements of the quality of the law governing such processing. While the collection and further processing of personal data are an

indispensable part of the functions of law enforcement authorities, there are, at the same time, significant inherent risks of abuse involved with a view to the exercise and protection of the rights and freedoms of individuals whose data are being processed. A sufficiently rigorous approach when assessing the quality of the law is therefore necessary. This is all the more so in the light of the developments referred to in my separate opinion in *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13, 62322/14, 24960/15, 13 September 2018, not yet final; paragraph 15 of that opinion), namely the degradation of respect for democratic standards and the rule of law, of which there is increasing evidence in a number of States. Again, without any suggestion that the present respondent State were a case in point in this regard, the Convention standards must nevertheless be considered in the light of the dangers deriving from such developments *vis-à-vis* the protection of our common human rights and fundamental freedoms.

6. With this in mind, I consider that the crux of the legal issues raised by the present complaint relate to deficiencies in the quality of the law rather than (merely) the issue of necessity. As will be addressed more specifically below, the domestic legal framework, on an extremely vague and unspecific basis, has allowed for the processing of sensitive personal data without effective safeguards. The crucial importance of the quality of the law in a context such as the present one can be highlighted, most simply, by noting that that the general principles of data protection law – such as those requiring that the processing must be necessary for the purpose of the processing, and that the data to be processed must be adequate, relevant and not excessive in relation to that purpose – become diluted, possibly to the extent of practical irrelevance, where the purpose itself is left without any meaningful definition or limitation.

B. Analysis

7. In the present case, the processing of personal data has its basis in common law, under which the police have the power to obtain and store information "for policing purposes", including for the maintenance of public order and the prevention and detection of crime (see paragraph 34 of the present judgment). Thus, there is no underlying statutory basis, and the basis in non-statutory law is about as vague as it can get. For the particular database in question, no further legal basis exists.

8. Regarding the purpose of the database, it has been said that "the records are held to help UK policing manage a future risk of crime" (see paragraph 14 of the present judgment). According to the Government's submissions to the Court, the information is kept "for policing purposes" and "includes information relating to extremism but also relating to public disorder that does not involve extremism". All of this remains, well, extremely vague and obscure. As regards the Code of Practice issued by the Secretary of State (see paragraph 40 of the present judgment), the definition of "police purposes" given therein finishes with a general reference to the performance of "any duty or responsibility of the police", and therefore fails to provide any further specificity.

9. Thus, clear rules governing the scope of the measures are lacking. The accessibility and foreseeability of the norms are therefore clearly deficient. As mentioned above, these features in themselves also dilute the relevance and effectiveness of the safeguards against abuse and arbitrariness deriving from the general data protection principles applicable by virtue of the Data Protection Act.

10. In this context, it is worth reiterating that the Court has held that it is not only essential to have clear, detailed rules governing the scope of measures, but also governing safeguards relating to the storage, use, duration of retention, access, as well as procedures for preserving the integrity and confidentiality of data and for their destruction. The Court has stressed that as there are various crucial stages at which data protection issues under Article 8 of the Convention may arise – namely during collection, storage, use and communication of data – what must be in place for each stage are appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and which prevent arbitrary and disproportionate interference with Article 8 rights (see *M.M.*, cited above, § 195, and *Surikov*, cited above, § 74).

11. In the present case, the Government have stressed that the information was kept for policing purposes and had been neither intended for disclosure, nor disclosed, to any third party. The majority in the Chamber also put weight on this argument (see paragraph 103 of the judgment). The Government have also emphasised in line with the domestic Supreme Court that the information had not been obtained by covert means.

12. Neither of these points, however, is sufficient to make any crucial difference in the present context and circumstances. While it is true that secret surveillance or covert intelligence-gathering, or the accessibility of personal data, and of sensitive personal data in particular, to third parties must, for obvious reasons, entail heightened requirements for the quality of the law, both in terms of the specificity of the legal framework and the robust nature of the requisite safeguards, this cannot mean that the absence of such features could justify a lax approach to those requirements, especially where the processing of sensitive data is concerned. In view of established European principles regarding the processing of personal data, the fact that the processing may be limited to the "internal" functions of public authorities, without data being made available to "external" third parties, or that the data do not originate from covert operations, are not decisive distinctions in terms of the required elements of protection. Nor do the facts that the data were collected in relation to events in public places, or that they comprised primary facts which were "in the public domain", such as a person's name and address, make any decisive or fundamental difference. It is well known that the need for protection of personal data often depends, quite essentially, on elements such as the context, combination, use and accessibility of such data (from the Court's case-law, see, for instance, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, §§ 134-137, ECHR 2017).

13. With these remarks, I would like to stress that the interpretation of relevant Convention standards should not evolve on the basis of criteria, or distinctions, that would give rise to unwarranted divergences in the approaches between data protection as conceived

under Article 8 and as conceived under specific instruments of international law in this field. As the Court has stated in other contexts, the Convention should be interpreted in harmony with the general principles of international law, and the Court should aim at a combined and harmonious application of relevant international instruments (see, for instance, *X v. Latvia* [GC], no. 27853/09, §§ 92-94, ECHR 2013).

C. Conclusion

14. The present case is, in my view, essentially an individual manifestation of the consequences arising from shortcomings in the underlying legal framework. The applicant, who had never been charged with any crime, nor accused of any violence, nor suspected of being directly involved in criminal activities undertaken by the group Smash EDO, and who had been assessed as not being a threat (see paragraphs 31 and 119 of the present judgment) ended up having personal data relating to his participation in demonstrations and trade union events, and thus to his peaceful exercise of the rights protected under Articles 10-11 of the Convention, kept on police records in a searchable database for an indefinite period. Even the existence of the database in question was not clearly acknowledged until the domestic proceedings in this case (see paragraph 98 of the present judgment). A subsequent review of matters relating to undercover police operations, prompted by allegations made by whistleblowers, also led to a review of the database on overtly obtained intelligence (see paragraph 13 of the judgment), resulting in the deletion of part of the data originally retained concerning the applicant. As pointed out by the applicant in his submissions, a system that must rely on whistleblowers, litigation and press disclosure to ensure proper conduct is not adequate in terms of protections against abuse or arbitrariness.

15. For the reasons set out above, I consider that it would have been appropriate for the Chamber to focus its analysis more thoroughly and consistently on the assessment of the "quality of the law" aspect of the case, because that is where the crux of the case lies, instead of leaving that issue open and resolving the case on the basis of the assessment of "necessity". In my view, the quality of the relevant legal framework was not adequate in a context such as the present one, and therefore the interference was not "in accordance with the law" within the meaning of Article 8 § 2. This finding is sufficient to conclude that there has been a violation of Article 8.