Case Comment: Catt v the United Kingdom: A lesson for the UK and European Court of Human Rights?

Dr Matthew White

Abstract

This comment considers the Chamber of the European Court of Human Rights judgment in *Catt v United Kingdom*.[1] This case concerned the applicant's complaint regarding the collection and retention of personal data which included their political views on a police 'domestic extremist' database. The Chamber unanimously held that Article 8 had been violated taking into account the nature of the personal data, the age of the applicant and the fact they had no history or prospect of committing acts of violence. Whilst the Chamber found that the collection of personal data had been justified, its retention had not, particularly considering the lack of safeguards.

Key words: data retention, Article 8, Article 11, policing, databases, extremism, personal data

1. Introduction

The 94-year-old applicant, Mr Catt, is a lifelong peace activist and a regular attender at public demonstrations.[2] In 2005, Mr Catt began to take part in protests by a group called Smash EDO whose objective was to close down the activities of a US arms company EDO MBM Technology Ltd. The protests involved disorder and a large police presence, though twice arrested, Mr Catt has never been convicted of any offence.[3] In March 2010, Mr Catt made a subject access request (SAR) under the Data Protection Act 1998 (DPA 1998) for any information about him that was held. The SAR disclosed 66 entries from a police 'Extremism database' collected from March 2005 to October 2009, mostly related to Smash EDO, but 13 entries relating to attendances such as at a Trades Union Congress conference in Brighton in 2006, at a demonstration at a Labour Party conference in 2007 and a pro-Gaza meeting in 2009. In the majority of cases, information about Mr Catt's name, presence, address, DOB, appearance and in one instance a photo was kept.[4] In August 2010, Mr Catt sought to have said information deleted, but the Association of Chief Police Officers (ACPO) declined to do without reasons.[5]

In November 2010, Mr Catt issued judicial review proceedings on the refusal to delete data for not being 'necessary' under Article 8(2).[6] In May 2012, the High Court[7] ruled that Article 8 was not engaged, and even if it was, interference with it was justified. In March 2013, the Court of Appeal,[8] however, saw differently in ruling that Article 8 had been interfered with and violated as the National Coordinator, (whose role it is to 'coordinate the UK police

[1] *Catt v the United Kingdom* App no. 43514/15 (ECHR, 24 January 2019).
[2] ibid, [6].
[3] ibid, [7-8].
[4] ibid, [9-10].
[5] ibid, [11].
[6] ibid
[7] *Catt v The Commissioner of Police of the Metropolis* [2012] EWHC 1471.
[8] *Catt, R (on the application of) v The Association of Chief Police Officers of England, Wales and Northern Ireland & Ors* [2013] EWCA Civ 192.

response to domestic extremism')[9] was unable demonstrate how this information provided any assistance. In March 2015, the Supreme Court[10] took a different view to the Court of Appeal, although accepting that Article 8 was interfered with, by a majority of four to one, ruled that Article 8 had not been violated. Lord Sumption giving the leading judgment argued that said measures were in accordance with the law due to the general application of the DPA 1998 and the specific application of statutory Code of Practice.[11] Lord Sumption with regards to proportionality, continued that political protest was protected by common law and Articles 10 and 11, but the retention of information, even those who are under no suspicion of criminal activity was justified. Lord Sumption surmised this by highlighting that the invasion of privacy was minor, as no intrusive procedures were used to record said information due to the public nature of activities. Lord Sumption continued that this was justified because this enabled the police to make a more informed assessment of risks/and threats to public order, to investigate any (or potential) criminal offences and to identify witnesses and victims and 'to study the leadership, organisation, tactics and methods of protest groups which have been persistently associated with violence.'[12] Lord Sumption felt that indiscriminate intelligence gathering was necessary and could only be judged in hindsight. Moreover, it was argued that information held about third persons did not carry such stigma of suspicion or guilt as it did not imply they were extremists. Finally, Lord Sumption noted that there was no prospect of the information being given to third parties, or used for political purposes, and the data was periodically reviewed for retention or deletion.[13]

2. Judgment

Before handing down its judgment, the Chamber acknowledged that the Government had communicated to it that there were four more entries relating to Mr Catt. The Government highlighted that the police could not explain why such entries were not disclosed earlier.[14] After acknowledging that Mr Catt's claim was admissible,[15] the Chamber proceeded and accepted that the measures did indeed interfere with Article 8, but questioned whether this interference as the Government had argued, was 'limited.'[16]

On the issue of whether the data collection/retention had been 'in accordance with the law', the Chamber highlighted its concern that 'collection of data for the purposes of the database did not have a clearer and more coherent legal base.'[17] However, the Chamber recognised that the framework for governing collection could not be considered in isolation from provisions governing retention and access, and thus proceeded to consider the regime holistically.[18] When discussing the retention of data, the Chamber highlighted similarities with *M.M. v the United Kingdom*[19] (which concerned the retention and disclosure of criminal record data) and some differences, notably, that *M.M* concerned *sensitive* personal data which it was acknowledged could have devastating consequences if disclosed,[20] moreover, it

[9] *Catt*, (n7), [5].
[10] *CATT and T, R (on the applications of) v Commissioner of Police of the Metropolis* [2015] UKSC 9.
[11] *Catt*, (n1), [25].
[12] ibid, [27].
[13] ibid, [27-29].
[14] ibid, [15-17].
[15] ibid, [73-79].
[16] ibid, [92-93].
[17] ibid, [99].
[18] ibid.
[19] *M.M v the United Kingdom* App no. 24029/07 (ECHR, 12 November 2012).
[20] *Catt*, (n1), [101-103].

could not be disclosed to third-parties.[21] Despite the Chamber having concerns about the ambiguity of the legal basis for the collection of Mr Catt's personal data, such as the loosely defined notion of 'domestic extremism' and the fact that said data could be retained indefinitely, they found it unnecessary to consider whether said measure was 'in accordance with the law' and opted instead to consider whether it was 'necessary in a democratic society.'[22]

The Chamber maintained that the database pursued the legitimate aim of preventing disorder or crime and safeguarding the rights and freedoms of others.[23] Moving onto the elements of a measure being 'necessary in a democratic society', the Chamber reiterated that it requires 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".'[24] The Chamber also observed that a margin of appreciation is left to the competent national authorities in this matter.[25] However, in dealing with the margin of appreciation first, the Chamber felt that it was necessary to intervene. Firstly, the Chamber noted that it 'considers significant that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection.'[26] The Chamber noted that at the domestic level, this was not a particular focus of the litigation as the Court of Appeal (though finding a violation of Article 8), did not consider that examining the specific principles of data protection would add anything to their analysis. Moreover, before the Supreme Court, Mr Catt did not pursue any specific data protection arguments, which in turn only referred to data protection more generally in the context of lawfulness. For the Chamber, however, the sensitive nature of Mr Catt's claim was a 'central feature' of the cases before the domestic courts as well as the Chamber.[27]

Although the position of the High Court on non-interference was rectified by the Court of Appeal and Supreme Court, the Government still maintained that retention was not systemic and the nature of the interference was limited. The Chamber sought to clarify.[28] The Chamber recalled previous case law in which '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.'[29] The Chamber ruled that although said previous cases concerned covert surveillance, it should be guided by that approach, especially since concerns relating to the ambiguity of the measures had been highlighted.[30] The Chamber also took into account the manner and timing of the disclosure that the fact that more personal data had been held on Mr Catt than revealed at the time of domestic proceedings.[31] The Chamber accepted there was a pressing social need (based on the legitimate aim) for the database, and therefore limited its consideration for whether there was a pressing social need with regards to the particular facts of Mr Catt's case.[32] The Chamber agreed that there was a pressing social need to collect Mr

[21] ibid, [103, 105].
[22] ibid, [107].
[23] ibid, [108].
[24] ibid, [109].
[25] ibid.
[26] ibid, [112].
[27] ibid.
[28] ibid, [113].
[29] ibid, [114].
[30] ibid.
[31] ibid, [115].
[32] ibid, [116].

Catt's personal data, and agreed that it is in the nature of intelligence gathering that the police first need to collect data before evaluating its value.[33] The Chamber also agreed with the domestic courts that the police had an obvious role to monitor protests of Smash EDO given their propensity for violence and potential criminality, thus even if Mr Catt himself was not suspected of being directly involved in the group's criminal activities, the police were justified in collecting his personal data given that he decided to align himself with Smash EDO.[34]

However, the Chamber was not prepared to accept that the retention of Mr Catt's personal data served pressing social need. The Chamber cited the absence of rules setting a definitive maximum time limit on the retention of such data**,** which put Mr Catt at the mercy of the highly flexible safeguards in the management of police information Code of Practice (MoPI). The Chamber reiterated that when a state puts such a system in place, the necessity of the effective procedural safeguards become decisive as those safeguards must enable the deletion of data once its continued retention becomes disproportionate.[35] The Chamber noted that Mr Catt's personal data could potentially be retained indefinitely as the six-year review intervals could not be said to have been conducted in any meaningful way, especially as they did not result in the deletion of any data,[36] in contrast to principle 4 of the Committee of Ministers' Resolution (CoMR) (74) 29.[37] The Chamber also cited the limited impact of requesting deletion, the later disclosure without explanation of additional data and the fact that some personal data concerning Mr Catt's involvement in non-violent protest was collected over six years ago and remains in the database despite the police and courts accepting that he did not pose a danger to anyone.[38]

Additionally, the Chamber highlighted their concerns with the absence of effective safeguards for personal data revealing political opinion, protected by Article 11. Mr Catt had attended events in relation to trade unions, this was important for the Chamber as Article 11 has special protections for trade unions. The Chamber also highlighted that the National Coordinator's definition of 'domestic extremism' referred to 'to collection of data on groups and individuals who act "outside the democratic process"' thus not even respecting their own definition as data pertaining to Mr Catt's 'association with peaceful, political events: such events are a vital part of the democratic process' was retained.[39] The Chamber considered 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".'[40] The Chamber also highlighted that principle 2 of the CoMR (87) had been violated in 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.'[41] The Chamber also took into account Mr Catt's age and was not persuaded by the Government's argument that

[33] ibid, [117].
[34] ibid, [118].
[35] ibid, [119].
[36] ibid, [120].
[37] ibid, [121] '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.'
[38] ibid, [122].
[39] ibid, [123].
[40] ibid.
[41] ibid, [124].

reviewing and deleting all entries relating to Mr Catt would be too burdensome.[42] This enabled the Chamber to conclude that Article 8 had been violated.[43]

3. Discussion

The Chamber's judgment is a welcome[44] reminder to the UK and its domestic courts of the importance of Article 8. It highlights the importance of monitoring and reviewing intelligence on a regular basis.[45] The Chamber's judgment supports a position (based on previous judgments by the Grand Chamber) previously made by myself that data retention amounts to or is akin to mass secret surveillance, (also agreed with by the Court of Appeal) and thus the same safeguards should apply.[46] This is important as:

> Given the technological advances since the *Klass and Others* case, the potential interferences with email, mobile phone and Internet services as well as those *of mass surveillance attract the Convention protection of private life even more acutely* (author's emphasis).[47]

Netpol noted that the Chamber's judgment may force UK policing to start confronting the growing international recognition that privacy is essential for other rights, such as freedom of expression and assembly.[48] It is just as Goold noted, that '[i]t is hard to imagine, for example, being able to enjoy freedom of expression, freedom of association, or freedom of religion without an accompanying right to privacy.'[49] Wachter takes this approach further by highlighting that privacy must be elevated above other rights because 'it is the basis for personal development and fulfilment and due to its position as an underlying, enabling requirement for the realisation of other human rights.'[50] Due to this support for other human rights, Scheinin argues that privacy 'forms the basis of any democratic society.'[51] Nowak underlined the dualist nature of freedom of association as it grants civil and political rights. With regards to the civil rights aspect, freedom of association protects against arbitrary interference by the State or private parties when, for whatever reason and for whatever purpose, an individual wishes to associate with others or has already done so. From the

---

[42] ibid, [125-127].
[43] ibid, [128].
[44] Saunders Law, 'European Court rules against UK in 'domestic extremism' protest database case' (6 February 2019) <https://www.saunders.co.uk/news/court-rules-against-protest-database.html> accessed 20 February 2019.
[45] Joanna Carty, 'Retention of data: Catt v The United Kingdom 2019, European Court of Human Rights' (29 January 2019) <https://www.weightmans.com/insights/retention-of-data-catt-v-the-united-kingdom-2019-european-court-of-human-rights/> accessed 20 February 2019.
[46] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1, 33-34.
[47] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [53].
[48] Netpol, 'It's Time to Close Down the Police's "Domestic Extremism" Databases' (5 February 2019) <https://netpol.org/2019/02/05/domestic-extremism-day-2019/> accessed 20 February 2019.
[49] Benjamin J. Goold, 'Surveillance and the Political Value of Privacy' (2009) Amsterdam Law Forum 1:4 3, 4.
[50] Sandra Wachter, 'Privacy: Primus Inter Pares Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights' (2017) Oxford Internet Institute < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514 > accessed 20 February 2019, 21.
[51] Martin Scheinin, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' A/HRC/13/37 (28 December 2009) <http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> accessed 20 February 2019, para 11.

political rights perspective, it is essential for the existence and functioning of democracy, because political interests can be effectively championed only in community with others (as a political party, professional interest group, organization or other association for pursuing particular public interests).[52] The civil and political rights aspect has been noted by the Grand Chamber[53] of the ECtHR, whilst also highlighting that 'on numerous occasions affirmed the direct relationship between democracy, pluralism and the freedom of association.'[54] The Grand Chamber has also noted 'the right to freedom of assembly is a fundamental right in a democratic society and…is one of the foundations of such a society.'[55] Article 8 and 11 interrelate in various ways, for example, the Grand Chamber has highlighted that 'forming an association in order to express and promote its identity may be instrumental in helping a minority to preserve and uphold its rights.'[56] Ethnic identity falls within the ambit of Article 8.[57]Additionally, Aston notes that there is a 'significant overlap between interference in privacy rights and those relating to the restriction of assembly.'[58] The Grand Chamber noted that personal autonomy (another facet of Article 8) 'must therefore be seen as an essential corollary of the individual's freedom of choice implicit in Article 11 and confirmation of the importance of the negative aspect of that provision.'[59] This not only demonstrates the importance of freedom of association/assembly for democracy, but how privacy is crucial to the exercise of this right.

Given the above mentioned, the reference to Article 11 highlighted that none of the domestic courts paid particular attention to the special categories of personal data which was as the Chamber highlighted, a central feature of the case. As Alvanou maintains, the Chamber took an important step towards protecting human rights when many countries counter-extremism/terrorism legislation has compromised civil liberties.[60] The reference to the chilling effect is also of utmost importance. This is where 'the fear of being watched or eavesdropped upon makes people change their behaviour, even behaviour that is not illegal or immoral.'[61] van der Hilst has noted that the 'blanket and indiscriminate retention of sensitive personal data over a longer period of time can have a *severe 'chilling effect'*' as this may 'reduce people's willingness to participate in public life, which is a loss for the democratic functioning of society (author's emphasis).'[62] Rob McDowall, member of the Equality Council, Chair of Welfare Scotland and Rapporteur and Equality and Human Rights

---

[52] Manfred Nowak, *UN Covenant on Civil and Political Rights. CCPR Commentary* (2nd rev. ed.). (Kehl am Rhein: Engel, 2005), 385.
[53] *Zdanoka v Latvia* App no. 58278/00 (ECHR, 16 March 2006), [115].
[54] *Gorzelik and Others v Poland* App no. 44158/98 (ECHR, 17 February 2004), [88].
[55] *Kudrevičius and Others v Lithuania* App no. 37553/05 (ECHR, 15 October 2015), [91].
[56] *Gorzelik and Others*, (n54), [93].
[57] *Aksu v Turkey* App nos. 4149/04 41029/04 (ECHR, 15 March 2012), [58].
[58] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) EJLT 8:1 <http://ejlt.org/article/view/548/730> accessed 12 March 2019. p4.
[59] *Sørensen and Rasmussen v Denmark* App nos. 52562/99 and 52620/99 (ECHR, 11 January 2006), [54].
[60] Maria Alvanou, 'Security Policy and the Right to Privacy' (13 February 2019) <https://www.jurist.org/commentary/2019/02/alvanou-security-right-privacy/> accessed 20 February 2019.
[61] Rozemarijn van der Hilst, 'Human Rights Risks of Selected Detection Technologies Sample Uses by Governments of Selected Detection Technologies' (2009) <http://www.detecter.bham.ac.uk/D17.1HumanRightsDetectionTechnologies.doc> accessed, 20.
[62] Rozemarijn van der Hilst, 'Ranking, in terms of their human rights risks, the detection technologies and uses surveyed in WP09' (2011) <http://www.detecter.bham.ac.uk/pdfs/17_4_human_rights_ranking_of_technologies.doc> accessed 12 May 2017.

Advocate[63] was alarmed by a 'very weird telephone conversation' with the police who were seeking information on protests and events in Scotland and any information from Facebook groups.[64] It transpired that police in Scotland had been phoning political activists amidst Brexit fears.[65] Kirsty Haigh who was also contacted by the police tweeted:

> The police just phoned me wanting information about any upcoming anti-Brexit activity. The [Police Liaison Officer] said he'd been *instructed to phone me every week. Deeply unsettling for the police to be breathing down the backs of campaigners like this* – who has instructed them to do this? (author's emphasis).[66]

McDowall regarded this as 'bizarre and deeply unnerving'[67] and a Green MSP, John Finnie hoped that the police would 'reflect on their approach as it's self-evident that it has concerned active citizens who've been contacted.'[68] However, Assistant Chief Constable Mark Williams defended the strategy.[69] Nevertheless, this strategy raises alarming questions such as, how was this personal data obtained, under which law, for what purpose, who has access and for what purpose, and how long is this personal data stored, what are the processes for securing and deleting said personal data?

On 19 March 2019, King College London's (KCL) Justice for Cleaners (JfC) Facebook group posted that a minimum of ten politically active KCL students were blocked from entering the University.[70] JfC continued that vague justifications were offered by security suggesting that the Metropolitan Police had advised KCL to ban (which included 'all campuses, libraries and cafes, and prevented students from attending exams, work shifts, classes and assessed presentations') all students who were considered a security threat on the basis of a visit from the Queen.[71] It was noted that the police also took the names of these students for their own purposes.[72] All students affected were core organisers 'of campaigns that have established themselves as effective, successful and resistant to university apathy and reaction' and were 'predominantly women of colour.'[73] A senior staff member of KCL when confronted by a student told them a list was compiled ahead of the Queen's visit based

---

[63] Rob McDowall, <https://www.huffingtonpost.co.uk/author/rob-mcdowall/?guccounter=1> accessed 13 March 2019.
[64] McDowall, Rob (Rob McDowall) "A very weird telephone conversation. Saying they are looking at if I have any events or protests planned in the coming weeks or if I was aware of any. Asking if I knew of any planned in any Facebook groups etc. What on earth?" 8 February 2019, 1:11 p.m. Tweet.
[65] Andrew Learmonth, 'Police Scotland question protesters amid fears of Brexit chaos' (6 February 2019) <https://www.thenational.scot/news/17411043.police-scotland-question-protesters-amid-fears-of-brexit-chaos/> accessed 21 February 2019.
[66] Haigh, Kirsty (Kirsty Haigh) "The police just phoned me wanting information about any upcoming anti-Brexit activity. The PLO said he'd been instructed to phone me every week. Deeply unsettling for the police to be breathing down the backs of campaigners like this - who has instructed them to do this?" 4 February 2019, 5:48 p.m. Tweet.
[67] McDowall, Rob (Rob McDowall) "Is this happening elsewhere or just in Scotland? This is bizarre and deeply unnerving." 8 February 2019, 1:22 p.m. Tweet.
[68] Andrew Learmonth, (n65).
[69] ibid.
[70] KCL Justice for Cleaners (19 March 2019) <https://www.facebook.com/permalink.php?story_fbid=2244276068991224&id=1264160307002810> accessed 22 March 2019.
[71] ibid.
[72] ibid.
[73] ibid.

on CCTV footage of protests.[74] This not only raises issues of Article 8, but it also raises issues under Articles 10 (freedom of expression), 11, 14 (freedom from discrimination) and potentially Article 3 Protocol 1 (the right to education). As of writing this article, an open letter has been sent to KCL demanding an explanation of what has occurred, an apology and a commitment to not conduct such activity again in the future.[75] This is a concerning if 'students are being placed under surveillance by their university – this is a place of learning, not a police state, and surveillance has a chilling effect on students' freedom of expression.'[76] Furthermore, these concerns are not limited to the actions KCL, but also the police given what this article addresses.

Another, albeit less extreme example educational institutions compiling lists affecting freedom of association and assembly is the recent protests by Cambridge University's students and academics[77] protesting the institutions (St Edmund's College) appointment of Noah Carl,[78] involved in eugenics, a false and racist pseudoscience.[79] Siddarth Soni highlighted how the College compiled a list of protestors by various means including CCTV and blocked them on Twitter.[80] The above mentioned clearly dispels Lord Sumption's view that the privacy invasion was minor, when in fact privacy (which is not the same as data protection) was not the only right that was important. It demonstrates a profound lack of understanding of how the mining of (sensitive) personal data and its uses have real life consequences on rights not limited to Article 8. It also demonstrates Lord Sumption's ignorance of the very law that was interpreted when a false analogy was made between biometric data and Mr Catt's,[81] when the latter would be classed as sensitive personal data by virtue of s.2(b) of the DPA 1998. Sumption's lack of awareness is telling, and even if in Mr Catt's case, there was no chilling effect, Solove highlights that that the value of protecting against chilling effects cannot simply be measured by its effects on individuals exercising their rights, but the harms to society because amongst other things, 'they reduce the range of

---

[74] Amandla Thomas-Johnson, 'Pro-Palestine students denied university access during Queen's visit' (20 March 2019) <https://www.middleeasteye.net/news/pro-palestine-students-denied-university-access-during-queens-visit> accessed 22 March 2019.
[75] Open Letter on the Surveillance, Profiling and Exclusion of Students, (20 March 2019) <https://docs.google.com/document/d/1iuemk5icuqOOilYlYPoiYfSLDqLYwYNsIAo81fATJMc/edit?ts=5c92637f> accessed 22 March 2019.
[76] Amandla Thomas-Johnson, (n74).
[77] Soni, Siddarth (Siddarth Soni) "Over 40 protestors (students and academics) gathered outside Senate House to protest the appointment of Noah Carl (London eugenics conf attendee) to a fellowship at @Cambridge_Uni apalled that Cambridge has been unable to take a stance against the appointment. Atleast @ucl did!" 11 March 2019, 1:06 p.m. Tweet.
[78] Jess Ma, 'St. Edmund's students protest on King's Parade calling for rescindment of Noah Carl's fellowship' (9 March 2019) <https://www.varsity.co.uk/news/17309> accessed 13 March 2019; No Racist Pseudoscience, 'Photos: Students Protest Racist Appointment at St Edmunds College' (29 January 2019) <https://medium.com/@notmyfellow/photos-students-protest-racist-appointment-at-st-edmunds-college-e1b7eaacc716?fbclid=IwAR1fharn7gjebIXmHwmotZHo9Uu6NQBCggsRta5iVxig8K7H1Ks3gelN_O4> accessed 13 March 2019; Ben van Der Merwe, 'No, objecting to Cambridge's appointment of a eugenicist is not about free speech' (20 December 2018) <https://www.newstatesman.com/politics/education/2018/12/no-objecting-cambridge-s-appointment-eugenicist-not-about-free-speech> accessed 13 March 2019.
[79] Howard Markel, 'Column: The false, racist theory of eugenics once ruled science. Let's never let that happen again' (16 February 2018) <https://www.pbs.org/newshour/nation/column-the-false-racist-theory-of-eugenics-once-ruled-science-lets-never-let-that-happen-again> accessed 13 March 2019.
[80] Soni, Siddarth (Siddarth Soni) "Oh and regarding how college treats its own students who are protesting racism, they have literally compiled a list of protestors from CCTVs etc and censored them (full matriculated members of the institution) from engaging on their social media!" 11 March 2019, 3:35 p.m. Tweet.
[81] *CATT and T, R*, (n10), [26].

viewpoints expressed and the degree of freedom with which to engage in political activity.'[82] The fact that Chamber had to point out that the nature of the personal data was a central feature of the case further highlights Lord Sumption's lack of understanding and awareness of the issues raised before him.

The Chamber's judgment also has implications beyond politically sensitive data. In 2012, the Divisional Court in *RMC and FJ v Commissioner of Police of the Metropolis and Others*[83]ruled that the retention of 19 million custody images for a minimum of six years was in violation of Article 8. The Home Office preferred application made deletions rather than manual because it would cost too much.[84] Not only would this constitute a continuing violation of Article 8 for failing to comply with the judgment in *RMC*,[85] the European Court of Human Rights (ECtHR) are not persuaded by arguments that the cost of a measure as being justification for the continuance of a violation.[86] In *Catt*, the Chamber noted that:

> [I]s 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* (author's emphasis).[87]

This serves to significantly strengthen the argument that reliance on cost for non-compliance with the Convention is not tolerated. This position has another layer of importance given the use of facial recognition technology on custody images, which are currently subject to legal challenges.[88] As the ECtHR once elucidated:

> A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image.[89]

The Chamber's judgment matters because, as Lord Touson, in the Supreme Court articulated:

> [I]n 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.[90]

---

[82] Daniel J. Solove, ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) San Diego Law Review 44 745, 746.
[83] [2012] EWHC 1681.
[84] Matthew White, 'Whose Mugshot is it anyway?' (2018) 4YHRL <https://www.hrla.org.uk/wp-content/uploads/2019/01/2018-4YHRL-final-version.pdf> accessed 20 February 2019, 35-36.
[85] ibid, 36.
[86] ibid, 36-37.
[87] *Catt*, (n1), [127].
[88] Matthew White, (n84), 39.
[89] *Reklos v Greece* App no. 1234/05 (ECHR, 15 January 2009), [40].
[90] *CATT and T, R (on the applications of) v Commissioner of Police of the Metropolis*, (n10), [69].

Netpol maintained that although this judgment poses an enormous challenge to public order policing in the UK, this will not stop the sheer volume of intensive and unnecessary overt surveillance gathering that routinely occurs at protests.[91] This issue is meticulously highlighted by the concurring opinion of Judge Koskelo joined by Judge Felici. Although agreeing with the finding of a violation, Judge Koskelo had misgivings with regards to the analysis of whether the interference with Mr Catt's rights were 'in accordance with the law.'[92] They recite the requirements which note that:

> 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.[93]

Given that the Chamber is guided by principles in case law regarding secret surveillance, it is important to note that it is essential to have clear, binding[94] detailed rules, especially as the technology available for use is continually becoming more sophisticated.[95] With regards to foreseeability:

> In its case-law on secret measures of surveillance, the Court has developed the following *minimum safeguards* that should be set out *in **statute** law in order to avoid abuses of power*: the *nature of offences* which may give rise to an interception order; *a definition of the categories of people liable* to have their telephones tapped; *a limit on the duration* of telephone tapping; the *procedure to be followed for examining, using and storing the data obtained*; the *precautions* to be taken *when communicating the data to other parties*; and the *circumstances in which recordings may or must be erased or destroyed*…
>
> Furthermore, there must be a measure of *legal protection* in domestic law *against arbitrary interference* by public authorities with the rights safeguarded by Article 8 § 1. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, *it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power*. Consequently, *the law must indicate the scope of any such discretion conferred on the*

[91] Netpol, (n48).
[92] *Catt*, (n1), concurring opinion of Judge Koskelo joined by Judge Felici, [1].
[93] ibid, concurring opinion of Judges joined by Judge Felici, [2].
[94] *Valenzuela Contreras v Spain* App no. 27671/95 (ECHR, 30 July 1998), [60]; 'For this purpose, the rules need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them.' *Catt and T, R (on the applications of) v Commissioner of Police of the Metropolis* [2015] UKSC 9, [11].
[95] *Roman Zakharov v Russia* App no. 47143/06 (ECHR, 4 December 2015), [229].

> *competent authorities* and *the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference*…(author's emphasis).[96]

Judge Koskelo noted that given that personal and sensitive personal data was processed, particular vigilance was called for in assessing the requirements of the quality of the law as there are significant and inherent risks of abuse.[97] This was all the more so in light of recent judgments on secret surveillance where there has been a degradation 'of respect for democratic standards and the rule of law, of which there is increasing evidence in a number of States.'[98] Judge Koskelo highlighted that the crux of Mr Catt's case related to deficiencies in the quality of the law rather than just necessity due to the domestic legal framework being extremely vague and unspecific which allowed the processing of sensitive personal data without effective safeguards.[99] The crucial importance of the quality of the law for Judge Koskelo was that it would highlight that general principles of data protection law (such as necessity of processing and data minimisation) had 'become diluted, possibly to the extent of practical irrelevance, where the purpose itself is left without any meaningful definition or limitation.'[100]

Judge Koskelo highlighted that the legal basis for processing personal data derived from common law, thus not having any statutory basis, and that the non-statutory basis was 'as vague as it can get.'[101] This is all the truer as the DPA 1998 does not provide a legal basis for the collection of said data[102] as it:

> [S]afeguards how data is processed but does not provide a legal base; it does not authorise or require the acquisition of data through this type of activity. It does not fulfil all the functions the ECtHR has ascribed to 'law' [discussed in more detail below], specifically it gives no indication of when and to whom intrusive measures might apply. So while it might provide some safeguards against abuse, on its own it is not enough.[103]

Thus, this again, highlights Lord Sumption's misunderstanding of data protection law and the failure to recognise the requirements of legality under Article 8. The purpose of the database was said 'the records are held to help UK policing manage a future risk of crime' for 'policing purposes' and included 'information relating to extremism but also relating to public disorder that does not involve extremism.'[104] Noting that this was still extremely vague and obscure, Judge Koskelo noted that MOPI's definition of police purposes finishes with 'any duty or responsibility of the police' and therefore had failed to provide further specificity.[105] Judge Koskelo maintained that clear rules governing the scope of the measures

---

[96] *Sefilyan v Armenia* App no. 22491/08 (ECHR, 2 October 2012), [125-6].
[97] *Catt*, (n1), concurring opinion of Judge Koskelo joined by Judge Felici, [5].
[98] ibid.
[99] ibid, concurring opinion of Judge Koskelo joined by Judge Felici, [6].
[100] ibid.
[101] ibid, concurring opinion of Judge Koskelo joined by Judge Felici, [7].
[102] Lorna Woods, 'Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places' (2017) Journal of Information Rights, Policy and Practice 2:1, 2.
[103] ibid, 15.
[104] *Catt*, (n1), concurring opinion of Judge Koskelo joined by Judge Felici, [8].
[105] ibid.

were lacking, the accessibility and foreseeability were also deficient and these features themselves diluted the relevance and effectiveness of the safeguards against abuse.[106]

In support of Judge Koskelo's position, it will be explained why in this instance the measure in question were not 'in accordance with the law' whilst also using the principles of secret surveillance case law. Firstly, the definition of 'domestic extremism' as the National Coordinator admitted, was not prescribed by law.[107] Thus, it ultimately had no legal basis, and therefore cannot be 'in accordance with the law' contrary to Article 8.[108] This definition, as the Chamber highlighted, was loosely defined and could lead to the indefinite retention. This does not provide sufficient clarity or provide adequate protection against arbitrariness. This is highlighted when sensitive personal data pertaining to trade union activity and peaceful demonstrations were collected, despite falling outside the definition of 'domestic extremism.' The Chamber highlighted that this did not even comply with the definition given, and if they were acting on the assumption that this definition was lawful, they should have found a violation of Article 8 for not even complying with domestic law.[109] Furthermore, given that it was highlighted that the authorities did not respect their own definition, it highlighted that the said definition was *not binding* and would too amount to a violation of Article 8.[110] Due to the highly arbitrary nature and use of the definition of 'domestic extremism', this in and of itself would also violate Article 8.[111]

With regards to purposes, if as the Government contended that personal data was collected for purposes of extremism and public disorder, what was the purpose of collecting Mr Catt's personal data with regards to trade union activity and peaceful demonstrations when it was also admitted he had no propensity for criminal activity? Principles 2 and 5 of the then DPA 1998 prevented the processing of data for incompatible purposes and retention for no longer than necessary for that purpose respectively. The Chamber highlighted that retention of Mr Catt's sensitive personal data, even that with respects to Smash EDO could not be justified, collecting said data on peaceful and political events highlighted the danger of an ambiguous approach and that it did not take into account the need for heightened protection of said data (see Sch 3 of the DPA 1998), it would seem that once again, domestic law had not even been adhered to, and thus would again violate Article 8.

With regards to 'police purposes', the ECtHR has previously noted concerns with laws that allow surveillance in 'respect of a very wide range of criminal offences'[112] as it would 'not provide adequate protection against abuse of power by the State'[113] e.g. where 'the nature of the offences which may give rise to such an order are nowhere defined.'[114] Police purposes does not in any way define the nature of offences which can justify collecting personal or even sensitive personal data. Moreover, it is '*unclear…who – and under what circumstances – risks having the measure applied to him or her in the interests of…*[and]…fails,

---

[106] ibid, concurring opinion of Judge Koskelo joined by Judge Felici, [9].
[107] Dominic Ruck Keene, 'Privacy and the peace protestor — an extended look' (30 January 2019) <https://ukhumanrightsblog.com/2019/01/30/privacy-and-the-peace-protestor-an-extended-look/> accessed 21 February 2019.
[108] *Copland v United Kingdom* App no. 62617/00 (ECHR, 3 April 2007), [48-49].
[109] *Mustafa Sezgin Tanrikulu v Turkey* App no. 27473/06 (ECHR, 18 July 2017), [60], [64-65].
[110] *Mitkus v Latvia* App no. 7259/03 (ECHR, 2 October 2019), [137].
[111] *Roman Zakharov*, (n95), [302-305].
[112] ibid, [244].
[113] *Iordachi v Moldova* App no. 25198/02 (ECHR, 10 February 2009), [53].
[114] *Kruslin v France* App no. 11801/85 (ECHR, 24 April 1990), [35].

nevertheless, to *define*… "public order" (author's emphasis).'[115] This highlights that the ECtHR does not simply accept reference to Article 8(2) as justification in and of themselves for interference. In *Doerga v Netherlands* the Dutch Government argued that tapping and retention of conversations[116] were justified on the grounds of public safety and the protection of the rights and freedoms of others.[117] Yet, when examining the law under 'foreseeability,'[118] the ECtHR noted they lacked both clarity and detail nor did it 'give any precise indication as to the circumstances' when measures would be applied.[119] This was regarded as not being 'in accordance with the law.'[120] It was problematic that the Chamber accepted Lord Sumption's claim of the necessity of indiscriminate data capture given the vagueness of policing purposes as highlighted above are virtually unfettered powers[121] and too would violate Article 8.[122] This is true as Judge Pettiti in *Kopp v Switzerland*[123] noted that surveillance 'must be used *for a specific purpose, not as a general "fishing"*'[124] exercise to bring in information. Given the lack of statutory basis, the unlawful and arbitrary definition of 'domestic extremism', the vagueness of the police purposes accompanied by its unfettered reach, even with the common law, cumulatively, this would result in a violation of Article 8 for not being 'in accordance with the law.'[125]

Judge Koskelo reiterated that it is not only essential to have clear rules regarding the scope of measures, but also governing safeguards related to storage, use, duration of retention, access, procedures for preserving the integrity and confidentiality of the data and their destruction.[126] There must at 'each stage [be] appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and which prevent arbitrary and disproportionate interference with Article 8.'[127] Judge Koskelo highlighted how the Chamber put weight on the Government's point that information was kept internally, and that the Government emphasised in line with the Supreme Court that information was not gathered covertly.[128] Judge Koskelo noted that this did not matter because '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.'[129] Judge Koskelo continued that data only being accessible internally 'are not decisive distinctions in terms of the required elements of protection' nor information gathered was in the public domain as the 'protection of personal data often depends, quite essentially, on elements such as the context, combination, use and accessibility of such data.'[130] The public domain argument is true as the ECtHR has previously held that information obtained overtly still interferes with Article 8,[131] and would thus trigger the necessary safeguards required. Regarding internal access, the

---

[115] *Iordachi*, (n113), [46].
[116] *Doerga v Netherlands* App no. 50210/99 (ECHR, 27 April 2004), [43].
[117] ibid, [36].
[118] ibid, [50].
[119] ibid, [52].
[120] ibid, [54].
[121] *Liberty v UK* App no. 58243/00 (ECHR, 1 July 2008), [64].
[122] ibid, [70].
[123] *Kopp v Switzerland* App no. 23224/94 (ECHR, 25 March 1998).
[124] Stephen Uglow, 'The Human Rights Act 1998: Part 4: covert surveillance and the European Convention on Human Rights' [1999] Criminal Law Review 287, 289.
[125] *M.M.*, (n19), [206-207].
[126] *Catt*, (n1), concurring opinion of Judge Koskelo joined by Judge Felici, [10].
[127] ibid.
[128] ibid, concurring opinion of Judge Koskelo joined by Judge Felici, [11].
[129] ibid, concurring opinion of Judge Koskelo joined by Judge Felici, [12].
[130] ibid.
[131] *Peck v United Kingdom* App no. 44647/98 (ECHR, 26 January 2003), [59].

Government and Supreme Court's position is not strictly true as para 4.8.2 of the MOPI permitted sharing with 'other persons or bodies within the UK or overseas,' thus the intention not to disclose to third parties becomes irrelevant as [i]t is the *potential reach of the power* rather than its actual use *by which its legality must be judged* (author's emphasis).'[132] MOPI permits sharing on the same vague 'police purposes' so long as it is reasonable and lawful to do so. Moreover, MOPI is not binding on third parties, nor is there a list of who is entitled to receive this information. Additionally, one cannot assume internal sharing had been compatible with Article 8.

For Judge Koskelo, Mr Catt's case was simply an individual manifestation of the consequences from the shortcomings underlying the legal framework.[133] This highlights a major problem with the Chamber's approach when it accepted that the creation and maintenance served a legitimate aim. Judge Wildhaber's *et al's*[134] concurring opinion in *Rotaru v Romania* stressed that even in the national security context:

> [T]here has to be *at least* a *reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate. To refer to the more or less indiscriminate storing* of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern *is … evidently problematic* (author's emphasis).[135]

Failure to establish a legitimate aim would result in a violation of Article 8.[136] The Chamber also failed in its analysis when assuming because the database served a legitimate aim, it also served a pressing social need. Necessary does not have the flexibility of an expression such as 'admissible,' 'ordinary,' 'useful,' 'reasonable' or 'desirable.'[137] In Mr Catt's case, the measures were not necessary or even useful, a more rigorous analysis would have questioned the system as a whole because Mr Catt's circumstances were just a symptom. Moreover, 'powers which can be used in an arbitrary or discriminatory way are not transformed to a condition of legality simply because they are of proven utility.' [138] Failing on the grounds of establishing a pressing social need would result in a violation.[139]

Although the reference to Article 11 and the chilling effect is most welcome, had the Chamber considered previous case law, it could have demonstrated more authoritatively its importance. In *Segerstedt-Wiberg and Others v Sweden*, the ECtHR has acknowledged that the *storage* of personal data related to *affiliations and activities* engages Article 11.[140] The ECtHR could, of their own motion (likely through Rule A1(1)),[141] examine what the stance under Article 11 would be.[142] In *Segerstedt* even though there was no evidence of a chilling effect on their political freedoms the ECtHR nevertheless considered that:

---

[132] *Beghal v DPP* [2015] UKSC 49, [102].
[133] *Catt*, (n1), concurring opinion of Judges Koskelo joined by Judge Felici, [14].
[134] Judges Makarczyk, Türmen, Costa, Tulkens, Casadevall, Weber and Lorenzen in a separate concurring opinion.
[135] *Rotaru v Romania* App no. 28341/95 (ECHR, 4 May 2000*)*.
[136] *Erményi v Hungary* App no. 22254/14 (ECHR, 22 November 2016), [37-40].
[137] *Handyside v United Kingdom* App no. 5493/72 (ECHR, 7 December 1976), [48].
[138] *Beghal*, (n132), [93].
[139] *Faber v Hungary* App no. 40721/08 (ECHR, 24 July 2012), [59].
[140] *Segerstedt-Wiberg and Others v Sweden* App no. 62332/00 (ECHR, 6 June 2006), [107].
[141] Rules of Court (14 November 2016) <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf> accessed 11 November 2017.
[142] *Shimovolos v Russia* App no. 30194/09 (ECHR, 21 June 2011), [72].

> [T]he *storage* of personal data *related to political opinion, affiliations and activities* that is deemed *unjustified for the purposes of Article 8 § 2 ipso facto constitutes an unjustified interference with* the rights protected by *Articles 10 and 11* (author's emphasis).[143]

Thus, the Chamber in *Catt* could have ruled similarly.

4. Conclusion

The Chamber's judgment in *Catt* is another lesson for domestic courts on issues concerning data retention. It was important and welcome that the Chamber sought fit to be guided by principles set out in cases concerning secret surveillance (as they amount to the same thing) and highlighted the importance of Article 11 and the chilling effect that can arise with collecting sensitive personal data pertaining to peaceful assemblies and associations. It is also important as this judgment makes it even more difficult for authorities to justify not deleting data for reasons in contravention of Article 8. However, it is unfortunate that the Chamber did not consider whether the measures were 'in accordance with the law' in great detail as they would have found for a variety of reasons, the current legal framework would violate it. Additionally, the Chamber failed to critically consider the 'domestic extremism' database in its entirety was a legitimate aim or served a pressing social need. The Chamber missed the opportunity to demonstrate the public/social/collective value of privacy[144] by focussing solely on Mr Catt's circumstances and not the system he was caught up in. The issue of databases will not go away, as the police seek to create a super database,[145] despite reports of the Metropolitan Police's Matrix database being argued to be discriminatory,[146] Her Majesty's Revenues and Customs adding millions of voices to a Voice ID database,[147] the use of Automatic Number Plate Recognition (ANPR),[148] the looming possibility of an ID system post-Brexit,[149] and even the European Union's (EU) attempts at interconnecting all centralised EU databases[150] (and its Member States enabling communications data retention

---

[143] *Segerstedt-Wiberg*, (n140), [107].

[144] Priscilla M. Regan, *Legislating Privacy, Technology, Social Values and Public Policy* (The University of North Carolina Press 1995); Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015), 228-229.

[145] Matthew White, 'Proposed police super-database breaks the law and has no legal basis – but the Home Office doesn't care' (9 October 2018) <https://theconversation.com/proposed-police-super-database-breaks-the-law-and-has-no-legal-basis-but-the-home-office-doesnt-care-104527> accessed 21 February 2019.

[146] Vikram Dodd, 'Met gangs matrix may be discriminatory, review finds' (21 December 2018) <https://www.theguardian.com/uk-news/2018/dec/21/metropolitan-police-gangs-matrix-review-london-mayor-discriminatory> accessed 13 March 2019.

[147] Rebecca Hill, 'Just keep slurping: HMRC adds two million taxpayers' voices to biometric database' (25 January 2019) <https://www.theregister.co.uk/2019/01/25/hmrc_voice_id_big_brother_watch/> accessed 13 March 2019.

[148] Automatic Number Plate Recognition <https://www.police.uk/information-and-advice/automatic-number-plate-recognition/> accessed 13 March 2019.

[149] Pater Walker, 'ID cards a possibility after Brexit, says UK immigration minister' (13 March 2019) <https://www.theguardian.com/politics/2019/mar/13/id-cards-a-possibility-after-brexit-says-uk-immigration-minister?CMP=Share_iOSApp_Other> accessed 13 March 2019.

[150] Teresa Quintel, 'Connecting personal data of Third Country Nationals Interoperability of EU databases in the light of the CJEU's case law on data retention' (28 February 2018) <https://orbilu.uni.lu/bitstream/10993/35318/1/Teresa%20Quintel%20Interoperability%20of%20EU%20Databases.pdf> accessed 13 March 2019.

legislation),[151] a critical analysis would have been welcome. Moreover, by failing to fully utilise Article 11 in the database context as in previous case law, this was an opportunity missed by the Chamber especially considering police in Scotland are contacting protesters using their phone numbers to gain information. Netpol maintained that the judgment represents a direct challenge to the very basis of the intelligence model used by political policing in Britain,[152] but unfortunately, this is not the case when the judgment is considered as it must be remembered that '[t]he dossier of private information is the badge of the totalitarian state.[153]

[151] IT-Pol, 'EU Member States plan to ignore EU Court data retention rulings' (29 November 2017) <https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/> accessed 13 March 2019.
[152] Netpol, (n48).
[153] *Marcel and Others v Commissioner of Police of the Metropolis and Others* [1991] 2 W.L.R. 1118, [1130].