HOW EFFECTIVE IS THE CURRENT LAW GOVERNING POLICE RETENTION OF DATA IN THE UK, AT BALANCING INDIVIDUALS' RIGHT TO PRIVATE LIFE UNDER ARTICLE 8 OF THE EUROPEAN CONVENTION OF HUMAN RIGHTS, WITH THE PUBLIC INTEREST OF SAFETY?

Maximillian Maynard[1]

Abstract

This article evaluates whether the law governing police retention of data in the UK, effectively strikes a balance in protecting individuals' right to privacy, with the public interest of safety. This evaluation explores academic commentary, case law, and legislative provisions, as well as recent historical context in the area. The thesis of the piece is that, despite recent improvements in the law that serve to protect individuals' rights to privacy, conferred by Article 8 of the European Convention of Human Rights, the legal framework in this area is still flawed and continues to disproportionately encroach upon this right. In its conclusion, the proposition is agreed with, citing recent case law that demonstrates indiscriminate, indefinite retention of personal data, and ineffective responses to, otherwise positive, court decisions.

Introduction

The most influential decisions regarding this debate are often handed down by the European Court of Human Rights, in 'individual vs state' cases. One major theme that spans across most arguments presented by the police, is that, retaining personal data plays an important role in the prevention and detection of crime, as it allows more rapid identification of individuals, and can assist in predicting criminal activity, amongst other things. As well as this, retaining personal data serves to protect the vulnerable, in employment circumstances. In contrast, Article 8 of the ECHR, guarantees the right to 'respect of private and family life',[2] which is often infringed, when personal data is retained. This infringement can be justified, if the measures taken by the police are proportionate, and not excessively detrimental to the individual in question; this 'balancing act' is truly central to the discussions in this article, and to

[1] Maximilian graduated with a First Class LLB (Hons) degree in Law

[2] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8

the initial question itself. Retention of some types of data may appear inconsequential; however, privacy is said to occupy an 'elevated position' in the hierarchy of rights, meaning its infringement may affect the enjoyment of other rights too, like freedom of expression.[3]

Through analysis of common law, legislative provisions and academic commentary, I attempt to summarise where the legal framework of data retention is currently, and assess its effectiveness. The proposal which I will attempt to prove, is that the current law operating in the UK, despite positive development in recent years, remains flawed and ineffective at fully protecting citizens' right to private life.

1 How do the police retain data in the UK?

The current law & police guidelines

In this section, I will define the current legislation in force in the UK, as well as summarise key guidelines, governing police activity. The law outlined in this article is accurate as of April 2020. It is crucially important to understand the current law, in order to accurately answer the question, as these provisions provide the framework around the police's powers to retain and process personal data.

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect across all EU member states, including the UK.[4] This regulation provides provisions regarding the processing of individuals' data, which data controllers must abide by. In the UK, the Data Protection Act 2018 became the legislation that domestically implemented this EU law, and defined the aspects of the EU law that were to be determined by member states.[5] Despite the UK's withdrawal from the European Union (EU), on 31 January 2020, existing EU law remained domestically enforced via the European Union (Withdrawal) Act 2018. Sections two and three of the Act outline that both EU-derived domestic legislation, and direct EU legislation, will continue to

[3] 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 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514> Date accessed 22 April 2020

[4] DLA Piper, 'UK: UNDERSTANDING THE FULL IMPACT OF BREXIT ON UK: EU DATA FLOWS', (23 September 2019) <https://blogs.dlapiper.com/privacymatters/uk-gdpr-brexit-flowchart/> Date accessed 13 December 2019

[5] Pinsent Masons, 'New Data Protection Act finalised in the UK' (25 May 2018) <https://www.pinsentmasons.com/out-law/news/new-data-protection-act-finalised-uk> Date accessed 13 December 2019

have effect and become domestic law, on and after exit day, respectively.[6]

Part three of the Data Protection Act 2018 is titled, 'Law Enforcement Processing', and outlines many significant rules surrounding the police's processing and retention of personal data. The Act lists six data protection principles, which every controller of personal data is responsible for, and must demonstrate compliance with.[7] Additionally, it defines that within the Act, the phrase 'the law enforcement purposes' are the purposes of the prevention, investigation, detection or prosecution of criminal offences.[8]

The first principle listed is that processing of personal data (for law enforcement purposes) must be lawful and fair. Lawfulness can only be fulfilled if the data subject has given consent to the collection for law enforcement purposes, or that the processing is necessary for the performance of a task for those purposes.[9]

The second principle stipulates that the purpose for the data processing must be specified, explicit and legitimate; adding further, that data must not be processed in a way which is incompatible with the purpose for which it was collected. This includes processing data for a purpose that falls outside the list of 'law enforcement purposes.'[10]

The next principle outlines that processing must be 'adequate, relevant and not excessive in relation to the purpose for which it is processed'.[11] This is followed with the requirement that all processed data must be 'accurate, and where necessary, kept up to date', adding that any inaccurate data must be 'erased or rectified without delay'.[12] This fourth principle also requires that there must be a clear distinction between different categories of stored data.

The penultimate data processing principle is that data must not be retained for any longer than is necessary, in achieving the specified law enforcement purpose(s) for which it was processed.[13] The sixth and final principle is that data should be

[6] European Union (Withdrawal) Act 2018, s 2 and 3
[7] Data Protection Act (DPA) 2018 s 34(3)
[8] ibid s 31
[9] ibid s 35
[10] ibid s 36
[11] ibid s 37
[12] ibid s 38
[13] ibid s 39

processed 'in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.'[14]

The Data Protection Act 2018 also describes the rights of access for a data subject. It states that a data subject is entitled to obtain: 'confirmation as to whether or not personal data concerning him or her is being processed, and where that is the case, access to the personal data and the information set out in subsection'.[15] The following section of the Act provides that a data subject has the right to have their data rectified if it is inaccurate, 'without undue delay'.[16] As well as this, it provides that a data subject has the right to have their data erased where it infringes any of the data protection principles outlined previously in the Act.[17]

Alongside this legislation, the College of Policing (the professional body for policing) have developed the Authorised Professional Practice (APP), which is the official source of professional practice for policing. Police officers are 'expected to have regard to APP when discharging their responsibilities'; its purpose is, to provide 'skills and knowledge necessary to prevent crime, protect the public and secure public trust'.[18] The APP provides guidance across a wide range of police issues, including the 'management of police information'. This section of the APP is the guidance detailed in the Home Office's (2005) publication, 'Code of Practice on Management of Police Information' (MoPI).[19]

The APP makes direct reference to the Data Protection Act 2018, stating that the procedures on review, retention and disposal of records, ensure compliance with the aforementioned data protection principles found in the Act. It clarifies that retaining every piece of data collected by officers is unlawful, and therefore provides guidance on the criteria to consider when deciding whether to retain data, and what data to retain. The APP states that review is an effective method of meeting the requirements

[14] ibid s 40
[15] ibid s 45(1)(a) and 45(b)
[16] ibid s 46(1)
[17] ibid s 47(1)(a)
[18] Anon, 'About us' (23 October 2013) <https://www.app.college.police.uk/about-app/> Date accessed 14 December 2019
[19] Secretary of State for the Home Department, 'Code of Practice on Management of Police Information' (July 2005)< http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf> Accessed 14 December 2019

of the Data Protection Act 2018, on lawful retention of personal data.[20][21] These reviews are, according to APP, to be 'practical', 'risk-focused' and as 'straightforward as is operationally possible';[22] as well as this, it states that 'the police service should have standard procedures in place for reviewing records and making accountable decisions on the retention or disposal of information'.[23]

Additionally, the Human Rights Act 1998 (HRA), states that it is unlawful for public authorities to act in a way which is 'incompatible with a Convention right'.[24] The Act defines a public authority as 'any person certain of whose functions are functions of a public nature…', which therefore includes the police.[25]

In summary, it is evident that there are extensive provisions governing how the police carry out their responsibilities regarding data retention. The law in this area is, for the most part quite recent, and originates from a range of sources, in the form of codes of practice, domestic legislation and EU law.

The concept of proportionality

In this subsection, the concept of proportionality will be discussed and defined, as it is a highly relevant, general principle of international human rights law. This concept is also referred to in many of the guidelines and statutes mentioned above. The HRA gives effect to the rights and freedoms guaranteed in the European Convention of Human Rights (ECHR), and imposes that domestic courts must take into account judgments from the European Court of Human Rights (ECtHR) in Strasbourg.[26]

The focus of this article surrounds Article 8 of the ECHR, 'the right to respect for his

[20] Anon, 'Information management – Retention, review and disposal' (23 October 2013) <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#scheduled-reviews> Date accessed 14 December 2019
[21] DPA 2018, s 37 and 39
[22] 'Information management – Retention, review and disposal' (n 19) Date accessed 14 December 2019
[23] ibid
[24] Human Rights Act 1998, s 6(1)
[25] ibid s 3(b)
[26] Simamba Bilika, 'Proportionality as a constitutional ground of judicial review with special reference to human rights', (2016) Oxford University Commonwealth Law Journal, 125-159 <https://www-tandfonline-com.plymouth.idm.oclc.org/doi/full/10.1080/14729342.2016.1244452> Date accessed 17 December 2019

private and family life, his home and his correspondence'.[27] This is a qualified right, meaning public authorities may only infringe upon it where it is 'in accordance with the law' and 'necessary in a democratic society'.[28] In the ECtHR, proportionality is one of the main guiding principles used when assessing authorities' actions, which infringe individuals' rights under the convention; actions which often stem from the legislation and guidelines outlined in 1.1 above.[29] Proportionality has been described as 'bedrock', within the ECHR and all EU law.[30]

Usually, before proportionality need be discussed in a case in the EctHR, the courts must satisfy preliminary questions about the disputed actions of the public authority in question. First the court must ask whether there has been an interference with a specific human right; followed by whether this interference can be justified. This justification can be tested by examining whether an infringement has basis in national law, called the legality test; and, whether said infringement has occurred 'pursuant to a particular legitimate aim or purpose', called the legitimate aim test.[31] Proportionality is then considered by assessing several factors: whether the measure in question is suitable to achieve the legitimate aim, whether alternative, less restrictive measures could have used to achieve the aim and finally, whether the measure caused excessive detriment to the individual, in comparison to the benefits gained from its execution. These tests could colloquially be called, the 'suitability', 'necessity' and 'strict proportionality' tests, respectively.[32]

It is unlikely that an authority would fail the suitability test, as only 'absurdly irrational' measures tend to garner this judgement.[33] Additionally, a quote from the judgment of *Dudgeon v United Kingdom* demonstrates the practical application of the 'strict proportionality' test mentioned above:
'On the issue of proportionality, the Court considers that such justifications as there are for retaining the law in force unamended, are outweighed by the detrimental

[27] Guide on Article 8 of the European Convention on Human Rights, page 12. <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> Date accessed 17 December 2019
[28] ibid
[29] Alexey Dolzhikov, 'The European Court of Human Rights on the Principle of Proportionality in 'Russian' Cases' (2011) Teise, <https://ssrn.com/abstract=2695159> Date accessed 17 December 2019
[30] Yutaka Arai-Takahashi, 'Proportionality', Oxford Handbook of International Human Rights Law (Oxford University Press 2013)
[31] ibid
[32] ibid
[33] ibid

effects which the very existence of the legislative provisions in question can have on the life of a person…'[34]

This quote highlights the pragmatic, realistic approach to the deliberations on the benefits and detriments of a measure, within the 'strict proportionality' section of the general principle. It can be noted that the first two tests in proportionality have more concrete guidance, for the courts to refer to in their decisions, whereas this third test's exact content is much more difficult to determine.[35] It has also been argued that this limb of proportionality undermines the rationale for the principle itself, as it relies too heavily on subjective reasoning, and does not add to a structure which can be replicated consistently between cases.[36]

In summary, the concept of proportionality can be used as a framework to assess the means, side-effects and sometimes even legitimacy of state aims.[37] Its use has been said to 'foster legal predictability, certainty and coherence', which are all desirable factors according to the rule of law.[38] It is, in more simplistic terms, a balancing act, between the interests of a community, and the rights of an individual.[39]

The concept or proportionality has been considered in numerous cases, both domestic and European, but is most recently and succinctly described in the case, *Bank Mellat v HM Treasury.*[40] The Supreme Court considered whether the interruption of the bank's dealings with the UK's financial sector was rational and proportionate in achieving the aim of the statute, to prevent nuclear weapons development in nations that pose a significant risk to the national interests of the United Kingdom. The court deemed that the distinction between Bank Mellat, and other Iranian banks operating in the UK's financial sector was arbitrary and irrational. Additionally, the measure itself was deemed disproportionate, as other analogous issues, with comparable banks, were solved using alternative sanctions. It was noted in the judgment that, 'a measure may respond to a real problem but nevertheless be irrational or disproportionate by reason of its being discriminatory in some respect

[34] Dudgeon v UK (1982) 4 E.H.R.R. 149
[35] Tor-Inge Harbo, 'The Function of Proportionality in EU Law' (2010) European Law Journal <https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-0386.2009.00502.x> Date accessed 29 December 2019
[36] ibid
[37] Andrew Legg, 'The Margin of Appreciation in Human Rights Law. Proportionality: Determining Rights' (Oxford University Press 2012)
[38] Yutaka Arai-Takahashi, 'Proportionality' (n 33)
[39] ibid
[40] Bank Mellat v HM Treasury [2013] UKSC 39, [2014] A.C. 700

that is incapable of objective justification'.[41]

Lord Sumption then went on to provide a four-stage test regarding rationality and proportionality, in cases of human rights infringements. The test was described as an 'exacting analysis of the factual case advanced in defence of the measure', to determine:

'(i) whether its objective is sufficiently important to justify the limitation of a fundamental right; (ii) whether it is rationally connected to the objective; (iii) whether a less intrusive measure could have been used; and (iv) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community'.[42]

The final limb of the test is of particular importance in addressing human rights restrictions, as it encapsulates the three limbs prior to it, and is at the heart of what 'balance' means in the context of the opening question, and the principle as a whole.

Proportionality's application, arguably, differs between the ECtHR and domestic courts in the UK. While the distinction is fine, it has been said that within the domestic setting, the principle creates discussion around issues which are increasingly political, as opposed to legal.[43] In turn, this begins to blur the lines between the separation of powers within the UK, namely the judiciary and the executive, as inevitably, judges must make 'value judgements' regarding the law.[44]

The ECtHR does not have the same constitutional boundaries to be aware of, so this issue does not apply in the same way, however, the European court must instead adhere to the principle of subsidiarity, which is 'closely bound up with … proportionality.'[45] This principle states that, 'the EU does not take action … unless it is more effective than action taken at national, regional or local level'.[46] UK judges have discussed the Strasbourg Court in extrajudicial speeches, and have repeatedly

[41] ibid [25]
[42] ibid [20]
[43] Adrienne Young, 'UKAEL Annual Lecture 2012 – Proportionality: the way ahead?' (*KSLR EU Law Blog*, 26 November 2012) <https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=284#.Xoxjpi2ZM1I> Date accessed 3 January 2020
[44] ibid
[45] Anon, 'Glossary of summaries' (*EUR*-Lex) <https://eur-lex.europa.eu/summary/glossary/subsidiarity.html> Date accessed 13 April 2020
[46] ibid

commented that the court 'should not second-guess domestic policy choices and judicial rulings', and does not go 'far enough' in granting Member States a margin of appreciation.[47] As well as this, it has been argued that the Court have 'strayed far away from giving the text the meaning as it was understood at the time when the Convention was drafted and adopted'.[48] Robert Spano, a judge in the Strasbourg Court, has recognised, and since responded to, these criticisms, describing the current climate as 'the age of subsidiarity'; he claims the Court is entering a phase of 'empowering' Member States to 'bring rights home'.[49]

Therefore, the principle of proportionality provides a method of assessment towards state action, through what is often referred to as a 'balancing exercise'.[50] While it has been criticised for its lack of rigidity and potential to cause judicial 'overstepping' of boundaries, it provides a flexible means in protecting individuals' rights on a case-by-case basis.

The 'Soham murders' & Bichard Inquiry Report

The Soham murders are contextually important to this discussion, as they are often linked with a sudden, society-wide, focus on the importance of effective vetting procedures, regarding criminal records. On 4 August 2002, two girls were murdered in Soham, by Ian Huntley; Huntley had been subject to eight separate sexual offence allegations, none of which surfaced during the vetting he undertook, prior to his appointment at Soham Village College.[51] The Bichard Inquiry was subsequently launched, with the aim of answering how and why these allegations had never been disclosed by the police. The Home Office's 2005 MoPI guidance on police information management was published as a direct result of this report, highlighting its impact on the legal landscape.[52]

The murders ushered in an 'almost universal acceptance' that the new system's 'enhanced certificates', which often consisted of 'hearsay and accusations', were the

[47] Robert Spano, 'Universality or Diversity of Human Rights? Strasbourg in the Age of Subsidiarity' (2014) Vol 14(3) Human Rights Law Review <https://academic.oup.com/hrlr/article/14/3/487/644292> Date accessed 13 April 2020
[48] ibid
[49] ibid
[50] 'The Margin of Appreciation in Human Rights Law' (n 40) Date accessed 5 January 2020
[51] The Bichard Inquiry Report
[52] *'Bichard Inquiry Recommendations Fourth Report'* (n 58)

way forward.[53] It has been highlighted that the principles of rehabilitation, proportionality and individual privacy, were largely neglected and ignored during this time, in favour of the new system.[54] Stewart Room, Head of Data Protection at Rowe Cohen Solicitors, wrote in January 2004 that, 'in a post-Soham world, it might be reasonable to conclude that the privacy angle will play a lesser role in the implementation of key child protection policies'.[55] The attitudes, reasoning and rationales expressed during this time, are still reflected in the more recent case law regarding data retention.[56]

2 Human rights case law on retention of data by the police

Catt v United Kingdom

In this section, significant cases involving retention of data by the police will be discussed, with the aim of providing a well-rounded picture on where the common law is currently, and how it has affected, and been affected by legislation and other guidelines and provisions.

Catt is a recent, landmark case surrounding data retention by the police and Article 8 of the ECHR. This case progressed all the way up to the ECtHR, having visited the Supreme Court and Court of Appeal previously. The case concerned Mr John Catt, whose personal data had been stored on the police's 'Extremism Database', despite having never been convicted of any offence.[57] Upon the applicant's initial data access request to the police, in March 2010, 66 entries mentioning him were provided, relating to his involvement with 'Smash EDO' protests, as well as records of his attendance at The Labour Party Conference and Trades Union Congress. Subsequently, in August that year, Catt requested that the Association of Police Chief Officers delete the entries mentioning him from information reports and nominal records; however they refused the request, offering no reasoning.

In January 2012, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (a body which assesses police forces' effectiveness and efficiency) published a report which expressed concern over the volume of data 'unnecessarily'

[53] ibid
[54] ibid
[55] Stewart Room, 'Data Sharing—Efficiency or Confusion?' (2004) 154 NLJ 51 at 55
[56] 'The Vetting Epidemic' (n 61)
[57] Catt v United Kingdom App no. 43514/15 (ECHR, 24 January 2019)

retained by the police.[58] Following this report, large quantities of nominal records and information reports were deleted from various police databases, meaning Mr Catt was now mentioned only six times.

The retention of these six data entries was still disputed, and was challenged via judicial review, in the High Court in February 2012. The case progressed to the Court of Appeal, who held that the interference with Catt's Article 8 rights was disproportionate and unjustified, on the basis that the police could not show that the stored information served the public interest in a sufficiently important way.[59] Plainly, the information provided no usefulness in predicting protesting tactics, attendance or nature.[60]

Again, the case was appealed, in the Supreme Court, where it was ruled in a 4:1 majority, that the retention of the six records was proportionate and in accordance with the law.[61] Lord Sumption's reasoning behind this conclusion was, in brief: to enable the police to make more informed assessment of risks, to investigate criminal offences where there have been any and identify potential victims and witnesses, and to investigate the hierarchical structure of protest groups which have been repeatedly involved with violence (as Smash EDO had).[62] Following this, the applicant took the case further, to the ECtHR.

The Strasbourg court unanimously agreed that there had been an interference with the applicant's Article 8 rights under the convention. The court then began deliberating on whether this interference was justifiable. Justification required the prescribed measures to be proportionate, that is, 'necessary in a democratic society', which would be fulfilled if they could be seen to answer a 'pressing social need'; the measures also had to be pursuant to a 'legitimate aim'.[63] Additionally, the authority had to provide sufficient reasoning to justify the encroachment. It was noted that a margin of appreciation should be left to national authorities in these scenarios, when discussing whether the measures taken were proportional to the 'need' they

[58] ibid [13]
[59] R. (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2013] EWCA Civ 192, [2013] 1 W.L.R. 3305
[60] ibid [44]
[61] R. (on the application of Catt) v Commissioner of Police of the Metropolis [2015] UKSC 9, [2015] A.C. 1065
[62] Jordan Owen, 'Retention of Data' (2019) 3 EHRLR, 321-324
[63] Guide on Article 8 of the European Convention on Human Rights, page 12 <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> Date accessed 15 January 2020

addressed.[64] In context, what this margin denotes, is that Strasbourg will not usually substitute its own decision for one of the domestic courts, even if the justification was provided using different reasoning than its own.[65] However, in this case the ECtHR deemed that this substitution was justified, as the information being retained included the applicant's political opinions; this type of information is classified as sensitive, meaning it is subject to greater levels of protection. Stemming from this, the ECtHR concluded that there had been a violation of Mr Catt's Article 8 rights.

Within the concurring opinion of Judges Koskelo and Felici, it was emphasised that the 'crux' of the case related not only to the necessity of the measures taken, but also the 'quality of the law'.[66] The 'policing purposes' provided by the Government, were described as 'extremely vague and obscure', specifically, the inclusion of information that was 'relating to extremism but also relating to public disorder that does not involve extremism.'[67] The concurring opinion was concluded with the observation that, the present case illustrated 'an individual manifestation of the consequences arising from shortcomings in the underlying legal frame-work'.[68] It was also pointed out that, as mentioned in the applicant's submissions, the fact that the review of the database, which resulted in the deletions of most nominal records, came from whisteblowers, shows inadequacy in 'terms of protection against abuse or arbitrariness'.[69] Therefore, the interference with the applicant's rights was not 'in accordance with the law', as it was required to be under Article 8.[70]

This case is highly relevant to the present discussion, as it reached its conclusion in 2019, making it a very current example of the Strasbourg Court ruling against the effectiveness of the legal framework surrounding data retention by the police. It has since had positive judicial treatment, solidifying its authority in the area.[71] The case has been called a 'resounding victory' for organisations campaigning against retention of private data by government bodies, and has been equally levelled, as a demonstration to the police, that 'internal procedures will need to be regularly updated

---

[64] ibid
[65] Anon, 'The Margin of Appreciation' (*Council of Europe*) <https://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp> Date accessed 24 January 2020
[66] *Catt* (n 67) [6] (Judge Koskelo)
[67] ibid [8]
[68] ibid [14]
[69] ibid
[70] ibid [15]
[71] Gallagher's Application for Judicial Review, Re R. (on the application of P) v Secretary of State for the Home Department [2019] UKSC 3, [2020] A.C. 185

and amended'.[72] Additionally, it has been described as an illustration of the Strasbourg Court's intent to 'champion the rights of data subjects', in a post-Brexit world, if GDPR were to become obsolete.[73]

MM v United Kingdom

The following case establishes that convictions and cautions fall within the scope of protection of Article 8, as they form part of a person's private life.[74]

In the case of *MM* the applicant raised complaints regarding the retention of her personal data, specifically, a caution from the police. [75] In November 2000 the applicant formally received a caution for child abduction; after she attempted to prevent her infant grandson's mother leaving for Australia, and disappeared with the child without parental consent, for two nights. Upon returning the child, the applicant was arrested, and in the presence of her solicitor, confirmed that she understood her actions to constitute child abduction. In the context, the Director of Public Prosecutions did not deem it within the public interest to initiate criminal proceedings. Instead, he indicated that a caution would be more appropriate.

In March 2003 the applicant was told, in response to a query, that the caution would remain on her record for five years, until November 2005. In September 2006, the applicant was offered employment as a care worker, however, this offer was subsequently withdrawn by the employers in consideration of her criminal records check.

The applicant then sought to challenge the acceptance of her caution in 2000, but was unable to do so; the Criminal Records Office cited in a letter, that where a person accepts a caution, they also accept their guilt to the offence. Additionally, they relayed that the law stipulating the time limit for retention of the caution, although correctly stated at the time, had since changed. The policy was now that, where the injured party is a child, records are kept on the system 'for life'.[76]

---

[72] Jordan Owen, 'Retention of Data' (n 72)
[73] ibid
[74] Elena Larrauri, 'Criminal record disclosure and the right to privacy' (2014) 10 Crim. L.R. 723-737 <https://www.researchgate.net/publication/289591252_Criminal_record_disclosure_and_the_right_to_privacy> Date accessed 28 January 2020
[75] MM v United Kingdom App no. 24029/07 (ECHR, 13 November 2012)
[76] ibid [13]

The applicant challenged the police's retention of her data in the ECtHR in 2012, claiming that her Article 8 rights had been infringed without sufficient justification. The court highlighted an 'absence of a clear legislative framework for the collection and storage of data, and the lack of clarity as to the scope, extent and restrictions of the common law powers of the police to retain and disclose caution data'.[77] The court also expressed concerns over the lack of any 'independent review mechanism' regarding decisions about retention of data, in the Police Act 1997, (the governing statute at the time).[78]

The court concluded that the safeguards in the data retention system were insufficient in ensuring that data would not be retained or disclosed, that could infringe an individual's right to a private life.[79] Therefore, the defendant's interference with said right could not be justified 'in accordance with the law'; the court unanimously held that there had been a violation of Article 8.[80]

In conclusion, this case once again demonstrated that retention without proper safeguarding, such as independent review, would violate Article 8. The court described the UK's police powers on retention of personal data as 'generous', and said that it was 'not surprising', that there were no previous judgments handed down, regarding individual challenges to police retention of criminal records data.[81] This generosity was attributed to the fact that, at the time, mere retention of data was not viewed by the domestic courts as an interference with Article 8, and if it was, this interference would be classified as 'minor'.[82] However, this attitude was challenged in *S and Marper v United Kingdom.*[83]

S and Marper v United Kingdom

S and Marper is another extremely influential Grand Chamber decision surrounding police retention of data.[84] This case was frequently considered in the judgment of

[77] ibid [206]
[78] ibid
[79] ibid [207]
[80] ibid
[81] ibid [170]
[82] ibid
[83] S and another v United Kingdom App nos. 30562/04 and 30566/04 (ECHR 4 December 2008)
[84] ibid

Catt v United Kingdom, when discussing the topic of whether measures were necessary in a democratic society, that is, whether they answer a 'pressing social need' and are proportionate to the pursued legitimate aim.[85]

The first applicant in this case was charged with attempted robbery, at the age of eleven, and had DNA and fingerprint samples taken from him pursuant to the Police and Criminal Evidence Act 1984. He was acquitted five months later. The second applicant was arrested and charged with harassment of his partner, he also had DNA and fingerprint samples recorded. Before pre-trial review, he reconciled with his partner, and the charge was never pressed. Both applicants subsequently requested their samples be destroyed, but were refused.[86]

This case is important largely due to the number of factors it established, or re-affirmed, in its judgment. The meaning of 'private life' within Article 8 was discussed, and was described as something that was not 'susceptible to an exhaustive definition'.[87] The court stated that, following previous case law, the 'systematic retention' of cellular samples, let alone their use, amounted to an interference with the rights defined in Article 8.[88] The court also reaffirmed that 'private life', covers the 'physical and psychological integrity of a person', including gender identity, links to family, rights to develop relationships with other human beings, and rights to your own image, amongst others.[89] Additionally, the court noted that DNA samples contain substantial amounts of personal information too, including such information that could be used to draw inferences regarding ethnic origin, making their retention 'all the more sensitive'.[90] In addition, the court also settled that retention of fingerprints was neither 'neutral or insignificant', and accordingly, constituted an interference with Article 8; any subsequent use of said data has no bearing on this fact.[91][92]

The court came to the decision that the interference, despite pursuing the legitimate aim of crime detection and prevention, was disproportionately detrimental to the applicants' private lives.[93] The court highlighted that the UK was the only member

[85] *Catt* (n 67)
[86] *S and another* (n 93)
[87] ibid [1]
[88] ibid
[89] ibid
[90] ibid [84]
[91] ibid [67]
[92] ibid
[93] ibid

state of the Council of Europe that 'systematically and indefinitely' retained DNA samples of individuals who had been acquitted, or who's criminal proceedings had been discontinued.[94] For these reasons, the national authority was seen to have 'overstepped any acceptable margin of appreciation' regarding the issue, and had failed to strike a 'fair balance between the competing public and private interests'.[95]

In its judgment, the court emphasised the contrast between Scotland and England ,Wales and Northern Ireland's procedures, regarding DNA profile retention. Despite being part of the UK, Scotland voted to allow retention of this type of data for three years in un-convicted persons, but only if the charge related to violent or sexual offences; these provisions were in line with the Committee of Minister's recommendations, which stressed importance on distinguishing between different kinds of cases.[96] This case serves to highlight the fact that the UK (bar Scotland)'s legal framework leans heavily on the side of the public interest, and neglects to acknowledge the importance of retaining personal data regarding private interests. Additionally, it demonstrates a disregard for the element of stigmatisation, and presumption of innocence of people who have not been convicted, as they are subject to the same treatment as convicted persons.[97]

The ruling in *S and Marper* was responsible for the Government's introduction of new legislation regarding DNA and fingerprints, including a six-year time limit on retention for persons arrested for, but not convicted of any recordable offences.[98] Section 64 of the Police and Criminal Evidence Act 1984, governing retention of DNA and fingerprint data, has been repealed and now forms part of the Protection of Freedoms Act 2012.

The decision in this case has also recently been followed in *Gaughran v United Kingdom*, a similar case regarding retention of DNA, fingerprints and photographs of a person, in Northern Ireland.[99] The ECtHR concluded that, following principles outlined in *S and Marper*, the 'indiscriminate' retention of DNA profiles, fingerprints and photographs, without reference to the seriousness of the offence, or 'real' chance of review, 'failed to strike a fair balance between the competing public and private

[94] ibid [110]
[95] ibid [125]
[96] ibid [110]
[97] ibid [122]
[98] Explanatory Notes to the Protection of Freedoms Act 2012, para 24
[99] Gaughran v UK App no. 45245/15 (ECHR 13 February 2020)

interests'.[100] This positive judicial treatment reinforces the principles established in *S and Marper*.

R. (on the application of C) v Commissioner of Police of the Metropolis

This case is largely similar to *S and Marper* (above), but focused on retention of custody photographs, of individuals' whose criminal proceedings had ceased. The first claimant had been arrested on suspicion of causing actual bodily harm to a police officer, however, the Crown Prosecution Service (CPS) had decided not to prosecute. The second claimant was arrested at the age of twelve, on suspicion of rape. He was bailed, but following further investigation, the decision was made to cancel the bail arrangement and halt further action.[101] Both claimants had DNA, fingerprints and custody photographs taken, and both requested their destruction due to seizure of respective proceedings, but the police decided the material should be retained. The commissioner contended that the police had acted according to policy, using 'Exceptional Case Procedure' in the ACPO's Retention Guidelines within the MoPI code of practice.[102] This procedure meant removal would be 'rare', and only gave rise to removal if 'the original arrest or sampling was found to be unlawful', which for these applicants, it was not.[103]

In its judgment, *S and Marper* was applied, to reiterate the principle that the mere retention of the photographs in question, amounted to an interference with the individual's rights under Article 8 of the Convention. While the court recognised that the MoPI Code of Practice provided a 'clear and detailed [legal] framework', they noted that there were still issues surrounding its application in terms of foreseeability and accessibility.[104] Additionally, the court stated that the MoPI code suffered from 'deficiencies of much the same kind as … *S and Marper*', in that there is no distinction between the convicted, and those who are either not charged, or charged and subsequently acquitted.

Therefore, once again, the court ruled that a fair balance between the competing public and private interests had not been struck. The retention of the claimant's

[100] ibid
[101] R. (on the application of C) v Commissioner of Police of the Metropolis, [2012] EWHC 1681 (Div Ct), [2012] 1 W.L.R. 3007
[102] ibid [19]
[103] John Lettice, 'Getting off the UK DNA database: ACPO explains how' (*The Register* April 2006) <https://www.theregister.co.uk/2006/04/26/dna_database_removal/> Date accessed 5 February 2020
[104] *R. (on the application of C)* (n 111) [46]

photographs amounted to an unjustified interference with their rights under Article 8.[105]

This case had a notable impact on the domestic law, with the majority in the Supreme Court holding that the ACPO's 'Exceptional Case Procedure' guidelines were unlawful, when read in conjunction with the HRA and ECHR.

Chief Constable of Humberside v The Information Commissioner

In this case, Chief Constables of five separate police forces in the UK appealed against the Information Tribunal's decision to have certain criminal convictions erased from the Police National Computer (PNC). The PNC is a police database used to 'facilitate investigations and sharing information of both national and local importance'.[106] The decision emanated from complaints made to the Information Commissioner, regarding disclosure of old, minor criminal convictions upon request by the Criminal Records Bureau (CRB), or in one case, by the individual making the complaint.

The police argued that deletion of convictions should only occur in exceptional circumstances, specifically, where convictions had been 'wrongly obtained'.[107] However, the tribunal contended that retention of the convictions at hand, had no value towards 'core' policing purposes, such as the detection and prevention of crime.

A notable detail of this case, was that one individual was told that her conviction would be erased on her 18th birthday, which subsequently, it was not. She claimed this contravened the first data protection principle of the 1998 Act, that data must be processed 'fairly and lawfully'.[108]

In rebuttal, the Chief Constables argued that to specify 'core' policing purposes, as the only justifiable purposes for retention of convictions, had no legal foundation in

[105] ibid [55]
[106] Anon, 'PNC – Police National Computer' <https://www.college.police.uk/What-we-do/Learning/Professional-Training/Information-communication-technology/Pages/PNC-Police-National-Computer.aspx> Date accessed 5 February 2020
[107] Chief Constable of Humberside & Others v The Information Commissioner & Another [2009] EWCA Civ 1079, [2010] 1 W.L.R. 1136
[108] DPA 1998, sch 1 para 1

the 1998 Act, nor that of the relevant EU Directive 95/46.[109] They argued that being able to supply information to others, such as the CPS, constituted a registered purpose for retention of the data; therefore, there could be no argument that the retention was excessive, nor being retained for longer than necessary.

The court allowed the Chief Constable's appeals, agreeing with their opinion, that retention need not be for 'core' policing purposes exclusively. They stated that, while the purposes for retention had to be lawful to fulfil the first data protection principle, they were not limited to 'core' purposes. The data controller was required only, to list their specific reason for retaining data, which in this case, were the purposes of 'vetting and licensing'.[110] For those purposes, all convictions were required to provide an accurate list to services such as the CPS and CRB.

The court also explained that, even if the narrower 'core' purpose approach was adopted, if it was the 'honest and rationally held belief', that retaining these convictions aided the police's work, 'retention of that information should not be denied' to them.[111]

Furthermore, the court stated that the EU Directive 95/46, explicitly permitted the retention of convictions, to enable the creation of complete criminal convictions registers. This permission made it a practical impossibility, for the retention to interfere with the rights of individuals under Article 8 of the ECHR, as both legal frameworks originate from the same source.[112]

This decision was controversial among legal commentators, due to its seemingly 'minimal' benefits to the police, at 'huge' cost to individuals.[113] Interestingly, *S and Marper* was distinguished in this judgment; it was deemed 'no authority for the proposition that a record of the mere fact of conviction engages article 8', as the nature of the information involved was 'quite different'.[114]

---

[109] Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L281
[110] *Chief Constable of Humberside* (n 117) [34]
[111] *Chief Constable of Humberside* (n 117) [43]
[112] ibid [81]
[113] Terence O'Conor, 'Does a recent decision mean some people will never escape past convictions?' (*The Law Gazette* November 2009) <https://www.lawgazette.co.uk/law/-does-a-recent-decision-mean-some-people-will-never-escape-past-convictions/52936.article> Date accessed 7 February 2020
[114] *Chief Constable of Humberside* (n 117) [80]

3 Further analysis

In this section, I will attempt to assess the impact of the cases above, with reference to the reasoning in their judgments. I will also draw on academic commentary around data retention and privacy, using it to develop a representation of the current state of the law, and discuss its merits and flaws.

Due to its contemporary nature, I will begin by discussing *Catt v United Kingdom*. Hypothetically, a ruling in favour of the Government in this case could have yielded severe negative consequences. It is widely recognised that there is 'significant overlap' between interference with the right to privacy and restriction to the right of assembly.[115] In *Catt*, The Equality and Human Rights Commission submitted, as third-party interveners, that the retention of the applicant's sensitive, political data, could have a 'chilling effect on legitimate political protests', which was agreed upon by the court in its judgment.[116][117] This 'chilling effect', in practical terms, means 'the fear of being watched or eavesdropped upon makes people change their behaviour, even behaviour that is not illegal or immoral'; consequently, 'people's willingness to participate in public life [would reduce], which is a loss for the democratic functioning of society.'[118][119] Evidently, police retention of sensitive political data has the potential to affect assembly, which in turn threatens a key aspect of democracy itself, 'active participation of the people'.[120] The decision reached by the ECtHR was especially valuable in this respect, as the sensitivity of the data concerned was not 'a particular focus' of the case throughout domestic proceedings; whereas, it was described as 'central' in Strasbourg.[121]

The Court chose to be guided by approaches taken in previous cases regarding covert surveillance, as they recognised similarity in that, state powers in the present

---

[115] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) Vol 8, No 1 European Journal of Law and Technology <http://ejlt.org/article/view/548/730> Date accessed 15 April 2020

[116] *Catt* (n 67) [123]

[117] ibid

[118] 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> Date accessed 18 April 2020

[119] 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> Date accessed 18 April 2020

[120] Larry Diamond, 'In Search of Democracy' (1st Edition, Routledge 2015) 33

[121] *Catt* (n 67) [109]

case were 'obscure' and created a 'risk of arbitrariness', especially in the context of quickly advancing technology.[122] This decision has been described as 'important and welcome', as it emphasised the significance of Articles 8 and 11 (the right to freedom of assembly and association), and the effect retaining sensitive data could have on them.[123] The Court's ruling supports the opinion that 'data retention amounts to or is akin to mass secret surveillance', reinforcing why rigorous safeguards must apply.[124]

While the Court recognised the need for caution, when ruling what information does or does not benefit the police, it stressed the necessity for methods of effective safeguarding of all data.[125] The Court were willing to accept that retention of the applicant's data may well have served a 'pressing social need' for a period after its collection, but highlighted an absence of definitive maximum time limits on this retention, and the reliance of the applicant on the effective application of the 'highly flexible' safeguards outline by the MoPI Code of Practice.[126] In this regard, the six-yearly reviews outlined by MoPI showed no evidence of being conducted in 'any meaningful way', as the data in question had been retained for over six years already, despite the agreement by the police and domestic courts, that Mr Catt 'was not considered a danger to anyone'.[127] The police's decision to retain the applicant's data therefore demonstrates arbitrariness, as it served no current policing purposes.

Despite the general praise for the Court's decision in *Catt*, it has also been criticised for failing to examine whether the measures taken were 'in accordance with the law'. Academic criticism directed at this aspect of the ruling runs parallel to the concurring opinion noted earlier, led by Judge Koskelo. The Court has been accused of 'focussing solely on Mr Catt's circumstances and not the system he was caught up in', as there are evident flaws in the legal framework, on a broader, deeper level; the present case has been described as a mere 'symptom' of underlying issues.[128] With the proposed introduction of a police 'super database', that would combine the Police

[122] ibid [114]
[123] Matthew White, 'Case Comment: Catt v the United Kingdom: A lesson for the UK and European Court of Human Rights?' (2019) Vol 3 Journal of Information Rights, Policy and Practice <https://www.researchgate.net/publication/333691554_Case_Comment_Catt_v_the_United_Kingdom_A_lesson_for_the_UK_and_European_Court_of_Human_Rights> Date accessed 18 April 2020
[124] ibid
[125] *Catt* (n 67) [119]
[126] ibid
[127] ibid [120-122]
[128] Case Comment: Catt v the United Kingdom (n 134)

National Database (PND), and PNC, the lack of a more rigorous analysis on the 'accordance with the law' aspect, seems like a missed opportunity, and may leave the door open for further cases in the future.[129]

Catt has also been noted to have implications on *R. (on the application of C) v Commissioner of Police of the Metropolis* (*R v Metropolis*), discussed above.[130] The Divisional Court ruled in *R v Metropolis*, that retention of custody photographs amounted to a violation of Article 8 rights; 19 million images were subsequently being held in contravention of the decision, and Article 8.[131] The Home Office responded to this ruling, by implementing a system that requires individuals to apply to the chief officer of the relevant police force, to have their photo removed.[132] The Home Office stated that manual deletion of these photographs, would 'cost a considerable amount of money to achieve which we believe would be a poor use of taxpayer's money'.[133]

While the Court's ruling serves to protect the right to privacy, this practical 'solution' was heavily criticised. The Biometrics Commissioner commented that the legality of the procedure being introduced, depended on the extent to 'which those individuals without convictions successfully make an application for deletion'; he later added, that evidence of past analogous procedures was 'not encouraging'.[134] As well as this, he noted that this process would involve 'a great deal of individual decision making', which could result in 'forces exercising their discretion differently thereby resulting in a postcode lottery'; these comments highlight the potential for arbitrary decision making, which would undermine its viability as a solution to *R v Metropolis*' ruling.[135]

The procedure was also condemned by The House of Commons Science and Technology Committee (the Committee), in their biometric strategy and forensic

---

[129] Matthew White, 'Proposed police super-database breaks the law and has no legal basis – but the Home Office doesn't care' (*The Conversation* October 2018) <https://theconversation.com/proposed-police-super-database-breaks-the-law-and-has-no-legal-basis-but-the-home-office-doesnt-care-104527> Date accessed 21 April 2020
[130] Case Comment: Catt v the United Kingdom (n 134)
[131] ibid
[132] Matthew White, 'Who's mugshot is it anyway?' The Young Human Rights Lawyer (2018) 4YHRL – p34
[133] ibid
[134] Paul Wiles, 'Commissioner for the Retention and Use of Biometrics, Annual Report 2016' (September 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644426/CCS207_Biometrics_Commissioner_ARA-print.pdf> Date accessed 21 April 2020
[135] ibid

services report. Although the Committee recognised the police power to retain images of persons who posed ongoing risk, it found the Government's solution 'unacceptable'; it noted, 'un-convicted individuals may not know they can apply for their images to be deleted', and would thus be given less protection than individuals who had DNA or fingerprint samples taken.[136][137] The Committee concluded by recommending that an automatic deletion system be implemented immediately, or, failing that, manual deletion should begin 'as a matter of urgency'; whilst also recommending that the Home Office explain the lawfulness of its current solution.[138][139]

Catt's ruling only stands to reinforce the criticisms outlined above. The quote, 'the Court is not convinced that deletion of the data would be so burdensome as to render it unreasonable', was supplemented with the statement 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.'[140]

These points reinforce the well-established policy of the courts, that potential monetary costs, or personnel commitment, are not valid justifications for the refusal to abide by the Court's ruling.[141]

In summary, it is clear that the decisions made in both *Catt* and *R v Metropolis*, serve to protect individuals' right to privacy, by questioning the arbitrary nature of the provisions surrounding how each applicant's data was retained. While *R v Metropolis* has led to the (principle) prohibition on indiscriminate retention of un-convicted people's custody photographs, *Catt*'s ruling calls for a review of national retention policies.[142]

---

[136] Science and Technology Committee, 'Biometrics strategy and forensic services; (fifth Report)' (2017- 19 HC 800) <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf> Date accessed 20 April 2020
[137] 'Who's mugshot is it anyway?' (n 142)
[138] Biometrics strategy and forensic services; (fifth Report) (n 146)
[139] ibid
[140] *Catt* (n 67) [127]
[141] Bouamar v Belgium App no. 9106/80 (ECHR, 29 February 1988)
[142] Anon, 'Retention of data: Catt v The United Kingdom 2019, European Court of Human Rights' (*Weightmans* January 2019) <https://www.weightmans.com/insights/retention-of-data-

Another recurring feature in the cases outlined above, is the 'indiscriminate' nature of data retention. The ECHR outlines in Article 6, that 'everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law', which is often dubbed the 'presumption of innocence'.[143] In *S and Marper*, the court noted the general rule, 'that no suspicion regarding an accused's innocence may be voiced after his acquittal'; while the court also recognised that retention of data after acquittal could not be equated with 'voicing suspicions', it stated that indefinite retention of the applicants' data (after acquittal) 'heightened the perception' that they were not being 'treated as innocent'.[144] Due to this, the 'risk of stigmatisation' was voiced as a 'particular concern' in the case.[145] The Court's idea that data retention cannot be equated to 'voicing suspicions' has been criticised, as the presence of un-convicted individuals' data, alongside convicted individuals' data, on the police database, lowers the presumption of innocence for both parties, and results in a difference of treatment to that of the rest of the population (i.e. those who are not on the database).[146]

Catt, R v Metropolis and *S and Marper* all involved retention of personal data for individuals who had never been convicted of a crime. Therefore, the risk of stigmatisation outlined in *S and Marper* applied in each case; for this reason, it can be strongly argued that the decisions reached in each case demonstrated protection for the individuals' rights to privacy, and were correctly made by the courts.

In contrast, *Chief Constable of Humberside v The Information Commissioner* (*Humberside*), ruled that retention and disclosure of old, minor conviction data was lawful, to facilitate the creation of accurate convictions records. While the nature of the data, and individual's conviction status, is clearly different in *Humberside*, all individuals involved in the appeal received their convictions at, or below, the age of

---

catt-v-the-united-kingdom-2019-european-court-of-human-rights/> Date accessed 22 April 2020

[143] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 6 (2)

[144] *S and another* (n 93) [122]

[145] ibid

[146] Michael Lwin, 'Privacy issues with DNA databases and retention of individuals' DNA information by law enforcement agencies: the holding of the European Court of Human Rights case S and Marper v. United Kingdom should be adapted to American Fourth Amendment jurisprudence', (2010) Information & Communications Technology Law 189-222 <https://www.tandfonline.com/doi/abs/10.1080/13600834.2010.49406> Date accessed 24 April 2020

twenty, including three minors; so why was the element on stigmatisation, outlined in *S and Marper*, not considered?[147]

Another notable contrast in judicial attitudes expressed in *Humberside* regarded the guarantee of deletion, made to one individual. In *MM v United Kingdom* (*MM*), the Court 'expressed concern' regarding a change of policy, which extended retention of the applicant's police caution indefinitely, contrary to previous assurances made to her.[148] It was noted that the acceptance of the caution (in *MM*), was 'on the basis that it would be deleted after five years'; this draws similarities with *Humberside*, where one individual was told the conviction would be removed from their records on their 18th birthday. The Court expressed a very different view in the present case, stating 'if it is fair to retain convictions under the new policy it does not become unfair to do so simply because the data subject was told of what the policy then was when being convicted or reprimanded'.[149] The disparity between the cases is explained by the fact that *MM* concerned a caution, whereas, *Humberside* concerned a conviction; while both terms come with the label of 'guilty', a caution constitutes an acceptance of guilt at the cost of 'waiving' fair trial proceedings, whereas a conviction is the result of such proceedings.[150]

Humberside helps to illustrate the difference in judicial treatment between conviction data, and other types of personal data. It seems that the courts' attitude towards conviction data is more aligned with the attitudes of the police; whereas in other personal data areas, it often falls on the side of the individual. The decision to allow retention of old, minor conviction data in *Humberside*, despite criticism for being unbalanced against the individual, is understandable due to the nature of the information; the bulk of the criticism regarding the decision should be directed towards the procedures on disclosure of this information, as opposed to its retention.[151]

Conclusion

From the cases discussed, it is clear that there have been numerous impactful

[147] 'The growth and permanency of criminal records with particular reference to juveniles' (n 124)
[148] *MM* (n 85) [205]
[149] *Chief Constable of Humberside* (n 117) [48]
[150] *MM* (n 85) [205]
[151] 'Does a recent decision mean some people will never escape past convictions?' (n 123)

developments on the law, in favour of protecting individual's right to private life, under Article 8 of the ECHR. These developments are increasingly important every day, as police technology is constantly becoming more advanced and wide-reaching. The extensive use of the PNC, PND, and proposition of 'super-databases' stands to highlight the importance of the decisions discussed in this essay. It is understandably in the public interest, for police to be able to fully dispense their responsibilities as effectively as possible, which is why the law must be cautious when deciding what is, or is not, of use to them, when detecting and preventing crime. However, the law must also ensure that the police do not infringe individuals' rights without sufficient justification and foreseeability.

Despite positive judicial decisions, protecting individuals' right to private life, the practical implementation of these, leaves much to be desired. The absence of an effective and meaningful method of independent review was present in *S and Marper*, *MM*, *Catt* and *Gaughran v United* Kingdom, despite more than a decade passing between the first and last cases respectively. The MoPI Codes of Practice, which outline independent review requirements, are not being followed, and have had criticism for lacking in foreseeability and accessibility, despite the clear framework they provide.[152] The concurring opinion in *Catt* also levelled multiple serious criticisms at the underlying framework governing data retention; the 'policing purposes' behind data retention were called 'obscure and vague', the database in question lacked statutory foundation, and the fact that a review, of the way police retained data, stemmed from whistle-blowers, demonstrated inadequacy relating to risks of 'abuse and arbitrariness'.[153]

This lack of implementation undermines the ruling in *R v Metropolis* as well; the Court deemed retention of custody photographs, of individuals who had not been convicted, to be unlawful. This ruling affected 19 million photographs, yet the Home Office chose to implement an application system for deletion, despite major criticism. This ongoing retention, due to individuals being unsuccessful in their application, or not having knowledge of said remedy, has been described as a 'continuing violation' of the ruling in *R v Metropolis*, demonstrating theoretical protection but practical violation.[154]

While the decision in *Humberside* indicates that the Courts' attitude towards retention

[152] *R. (on the application of C)* (n 111) [45]
[153] *Catt* (n 67) [14] (Judge Koskelo)
[154] 'Who's mugshot is it anyway?' (n 142)

definitively changes regarding conviction data, it does nothing for the uncertainty of other data categories.

The contemporary decisions in *Catt* and *Gaughran v United Kingdom* highlight that, despite progress being made in terms of protection of the rights of the data subject, the legal framework surrounding data retention remains flawed. They illustrate a worrying reliance by individuals on the principle of proportionality being applied in court, and not on the legislative provisions themselves; this clearly indicates that the current law fails to strike an effective balance, between the competing public interest of retention, and private interest of the protection of rights conferred by Article 8, in its sole operation.