Northumbria
University
NEWCASTLE

EUROPEAN JOURNAL OF CURRENT LEGAL ISSUES, VOL 22, NO 1 (2016)

'Being on our radar does not necessarily mean being under our microscope':The Regulation and Retention of Police Intelligence

Jamie Grace (Sheffield Hallam) and Marion Oswald (Winchester) [1].

Cite as: Grace, J. and Oswald, M. " 'Being on our radar does not necessarily mean being under our microscope':The Regulation and Retention of Police Intelligence", (2016) 22(1) EJoCLI.

1. INTRODUCTION

Our article "is concerned with the systematic collection and retention by police authorities of electronic data about individuals" [2]. This piece will address the use by the police in the United Kingdom (UK) of a series of databases, which retain information concerned with risks and records of criminality. The more notable of these databases do so with respect to police 'intelligence' (a term for which we explore a number of conceptual definitions below). The doctrinal development as a prompt for this piece was the recent decision in the Supreme Court in the case of *R (Catt and T) v Secretary of State for the Home Department* [2015] UKSC 9. This failure of two conjoined attempts through judicial review to have information thoroughly deleted from police databases, in relation to two rather different sets of circumstances and policy pressures, is a landmark judgment in the surveillance and privacy law field as a whole. The judgment of the Supreme Court in *Catt* is discussed in detail in a later Part of this piece. Suffice to say, for a quick introduction to the case, that *Catt* in the Supreme Court was a successful appeal by the Metropolitan Police, in the form of a 4-1 split judgment in their favour. John Catt ultimately lost his case after seeking the deletion of text-based records from databases operated by a police unit with a national anti-extremism intelligence remit; a unit commonly known as the National Domestic Extremism Unit, and now known as the National Domestic Extremism and Disorder Intelligence Unit [3].

To signpost the structure of the piece as a whole; first we aim here in Part 1 to give an introduction to some of the tensions that arise between privacy and human rights, versus police efficacy and operational pressures, in the context of intelligence gathering, analysis and retention. In Part 2, we move on to consider the concepts of information and analysis as comprising 'police intelligence' found in some of the academic literature as it currently exists on the topic. Part 3 of this piece in turn provides a short review of concepts and practices in relation to electronic intelligence databases in operation by the police more broadly, and across different police jurisdictions and cultures; while Part 4 sees us address the police use of intelligence databases in the UK context more specifically. Parts 5, 6 and 7 in turn see us address and analyse police intelligence retention and regulation as a human rights issue; the recent Supreme Court decision in *Catt*; and then give a broader commentary and critique of the Supreme Court decision in *Catt*. In Part 8 of this piece we evaluate some recent changes to guidance on the retention and deletion of police records made following the decision by the Supreme Court in *Catt*. Concluding our piece, in Part 9, we highlight some conclusions and recommendations we feel we can make as to i) the shifting and advancing realities of police database technology and surveillance through electronic records generally, ii) definitional and doctrinal problems presented by varying concepts in play with regard to what is meant by 'police intelligence', and iii) the need for a single national regulator in the field of police intelligence more generally.

As wider background to the subject matter of this article, it is worth summarising the structural set-up of policing within the UK at present. England and Wales is divided into 43 independent county or multi-county police forces, each headed by a Chief Constable and overseen by an elected Police and Crime Commissioner (or the Mayor's office in London). Pursuant to common law and the vast body of Police Act legislation, each Chief Constable has significant powers devolved to him to discharge his duties. The National Crime Agency, again a separate organisation, leads on the investigation of serious and organised crime, including economic crime, cybercrime and child sexual exploitation. Further police organisations exist for certain dedicated functions such as the Royal Parks Police and the British Transport Police. In addition, there are a small number of specialist national police units, primarily within the Metropolitan Police, of which the above mentioned Extremism Unit is one. By far the largest of these specialist national units (although limited to England & Wales) is the Counter Terrorism Command (SO15) which has the lead for the detection, investigation and disruption of terrorism threats, domestic extremism, and sensitive national security police investigations. SO15 works closely with the UK's Security Service (MI5) and Secret Intelligence Service (MI6) which both have remits involving national security but neither have executive powers of arrest. Policing in Scotland and Northern Ireland is a devolved matter, each having a single police force, although with national security remaining a reserved matter for the UK Parliament.

Cases dealing with issues of the regulation of police intelligence are a distinct body within the common law. Claims brought by those who would challenge police discretion in the 'processing' of their of 'personal data' often see individuals draw upon a mixture of data protection law and human rights law to argue that one or more elements of the process of the gathering, retention and sharing of the information that identifies them within a body of police intelligence is unlawful. For instance, the recent decision of the UK Supreme Court in *Catt* dealt with information retained on the National Special Branch Intelligence System (including the database known as the Domestic Extremism Database); focused on the retention (and availability for analysis) of information connected to 'the planning or commission of crimes motivated by a political or ideological point of view.' [4] Another high-profile, recent decision of the Supreme Court in *JR38* questioned, and ultimately accepted, the lawfulness of sharing surveillance images of a group of young people involved in sectarian public disorder in Northern Ireland, via publication of those images in local newspapers [5]. This had been done by the Police Service of Northern Ireland in

order to identify certain teenage participants in that public disorder, and to thus further enable the police and local community groups to approach the young people concerned to intervene and try and steer them away from a course of more violent sectarianism [6].

Judgments from the Investigatory Powers Tribunal and the High Court [7], as well as a number of independent reports and studies[8] , continue to explore the rolling politico-legal debate over the exact extent to which the electronic surveillance powers of the security services, the police and some other public authorities in the UK should run, whether relating to the mass or 'bulk' interception of communications or the more targeted and investigatory access to telephone and internet records. But our overall aim is to address the extent to which UK and European human rights law contributes to the effective regulation of police 'intelligence' databases built up from information obtained through more 'direct' investigatory actions by the police. These might include filming, photographing or otherwise recording (whether covertly or overtly) individuals taking part in legitimate public protest, or those engaged in public disorder or violence, recording information about an individual provided by an informant, or noting information about an individual mentioned in documentary material (that might be publicly available). In this piece we will explore the retention of intelligence by the police as a human rights issue with particular focus given to the decision in *Catt*. We regard this decision as representing a step-change in judicial treatment of the collection of intelligence, in the way that an individual's (limited) rights to privacy (and further (as illustrated by *Catt*), freedom from long-term surveillance as an element of a right to protest, and thus as part of a connected right to freedom of expression[9]) will be regarded when wider and long-term law-enforcement needs have been prayed-in-aid. We conclude that the lack of definition around the term 'intelligence', reported inconsistency of application between police forces and the 'subjectivity' of current case law are all unhelpful - in terms of legal certainty, public trust and confidence, and for the decision-making process undertaken by the police themselves - and we explore a number of potential solutions.

2. EXPLORING CONCEPTS OF INFORMATION AND ANALYSIS AS COMPRISING 'POLICE INTELLIGENCE'

Bearing in mind the increasing emphasis in the UK on 'intelligence-led policing', [10] the terms 'intelligence' and 'database' deserve consideration at this point. In the policing and national security contexts, the term 'intelligence' is used fluidly to describe a type of information collected, and also to describe conclusions from the analysis of information. The College of Policing (the professional body for policing responsible for developing professional standards) describes intelligence as 'collected information that has been developed for action. It may also be classified as confidential or sensitive.' [11] The recent HMIC report *Building the Picture* (which assessed the current effectiveness of police systems for recording and disseminating of information in the light of data sharing failures) commented that 'not all information is classified as intelligence, but all intelligence is a form of information.' [12] An example of information might be the fact that a person lives at a particular address; this information might become intelligence if it becomes known that such address has been the location of criminal activity such as drug dealing. HMIC continue on to comment that 'the categorisation of information and intelligence is a fluid process and that individual pieces of information and intelligence need to be reviewed on a regular basis to ensure that their categorisation remains appropriate to the then current circumstances.' [13] Police intelligence may include typical forms of 'criminality information' such as past allegations or spent convictions in circumstances where such information forms an important or the only indication of a risk posed by an individual.

The above definitions tend to focus on information itself, rather than the results of analysis of information (although the HMIC definition implicitly acknowledges the need for analysis). It is clear that 'intelligence' is often taken to mean a conclusion that has been drawn by such analysis, or by bringing together two or more pieces of information. In the United States, the Department of Justice considers it a mistake to equate 'information' with 'intelligence'; intelligence is instead 'information plus analysis.' According to this definition, 'Intelligence is not what is collected; it is what is produced after collected data is evaluated and analysed.' [14] The website of the UK's Security Service, MI5, also (implicitly) acknowledges this link between the piece of information and an added ingredient of *analysis*: 'by gathering secret intelligence, we seek to obtain detailed knowledge of target organisations, their key personalities, infrastructure, intentions, plans and capabilities.'[15] The Authorised Professional Practice (APP) as produced by the College of Policing defines the deliverables resulting from analysis as 'intelligence products', which could be strategic or tactical assessments, or subject or problem profiles. [16]

In *Catt*, Lord Sumption commented on the link between intelligence and analysis, observing that:

"Most intelligence is necessarily acquired in the first instance indiscriminately. Its value can only be judged in hindsight, as subsequent analysis for particular purposes discloses a relevant pattern. The picture which is thus formed is in the nature of things a developing one, and there is not always a particular point of time at which one can say that any one piece in the jigsaw is irrelevant." [17]

We could interpret this comment as meaning that all information acquired could potentially be intelligence and therefore the circumstances in which it should be deleted would necessarily be narrow. It is worth noting that, as well as "intelligence" being ill-defined, the term 'analysis' itself can be applied to both the application of statistics to data and to assessing multiple sources of information to derive conclusions. The College of Policing takes the wider approach. According to the APP guidance documentation produced by the College, analysis is what 'identifies patterns in information enabling the analyst to draw inferences from them so that operational decisions can be made on further actions to take' which might include enforcement, further information gathering or implementing a crime prevention strategy. [18] The national police decision-making model, as originally modelled by the National Police Improvement Agency, and now promulgated by their successors, the College of Policing, recognises intelligence gathering, sifting and analysis as the bedrock of a decision making model [19].

Our brief review in this Part of our piece has highlighted differing views of the nature of intelligence. Intelligence could be, as in Mr Catt's case, the noted association of an individual with others who have committed crimes, or it could be the product of analysis, 'to provide further leads in investigations, to present hypotheses about who committed a crime or how it was committed, to predict future crime patterns, and to assess threats facing a jurisdiction' and thus, coming to conclusions, developing inferences, and making recommendations for action (much of which will of course be done in secret).[20] These are not mutually exclusive and different types of intelligence could have differing levels of potential privacy harm from minimal to significant.

In following Parts of this article, we will consider whether this lack of clarity has contributed to the difficulties of regulation in this area. While there is an argument that a clearer (statutory) definition of intelligence would be beneficial, there is a risk that the fluid nature of information versus intelligence would make that an impossibility, and indeed detrimental to the proper consideration and analysis of information, and subsequent actions. As MI5's Director General, Andrew Parker, has said, 'Knowing of an individual does not equate to knowing everything about them. Being on our radar does not necessarily mean being under our microscope.' [21] It could be said that the *Catt* decision has effectively acknowledged and approved this point with implications for the regulation of intelligence (in the wider sense) in the future.

3. CONCEPTS AND PRACTICES IN RELATION TO ELECTRONIC INTELLIGENCE DATABASES

Before we progress much further in our regulatory and legal discussion, we must place some focus on electronic intelligence databases. At its most basic, a database is merely a record-keeping tool, a way of structuring or organising data. Nowadays, in their most sophisticated form, databases serve as aggregators, producing large databases in terms of breadth and depth or by assembling a number of distinct databases. [22] New search and retrieval techniques enable the extraction and combination of information from disparate locations, enabling 'deep profiles' of individuals to be built up.[23] Such databases go some way to allowing the police to spot patterns which may otherwise attract negative press and public opinion of the police's apparent inability to identify and prosecute repeat offenders. These techniques give electronic databases their power from a policing perspective, subject to the accuracy and completeness of information included, [24] and conversely contribute to the privacy concerns around their use. 'Increasingly sophisticated mathematical and statistical techniques have made it possible to extract descriptive and predictive meanings from information that goes well beyond its literal boundaries'; giving Nissenbaum some concern about the 'unbounded confidence' placed in the potential of information analysis to solve social problems. [25] At its most extreme, emerging data mining and 'Big Data' analysis techniques could become an example of 'a new animism' as Hildebrandt has put it, of 'mindless data-driven agency'[26] potentially reducing the policing function to an algorithmic one. As acknowledged recently by the Independent Surveillance Review, 'opinions are divided as to how serious an intrusion into privacy each different stage of data acquisition, filtering, retention and eventual human analysis is.' [27] Despite this, it is generally accepted that privacy issues result not only from the subsequent analysis and use of the information but from the initial data collection.

We assume it is generally accepted that it is vital that UK human rights law treats with great rigour the retention and the sharing or disclosure of those records compiled about individuals by the police, and by their 'partner' organisations. Indeed, we regard the nature of police record-keeping as a classic example of the consideration of civil liberties against tensions over public safety, fears of social harms, and state security: often prompted by (perceived or real) risks of criminality, extremism, and terrorism [28].

As such then, in contemporary scholarly and popular discourse, surveillance is a human rights issue, and so too then is the issue of the creation and the use of police databases. This piece is not able to do justice to explorations of why privacy, in the face of surveillance, can be considered a human right, even if 'qualified' as an element of the right to respect for private and family life under Article 8 ECHR - nor does this piece seek to justify the assumption made on our part that privacy is valuable, and should be protected to an appropriate extent from state (including police) intrusion (which can occur, we feel, through surveillance in the form of databases and records-keeping) [29]. While we assume that this variant of a 'right to informational self-determination' [30], as an element of privacy, must be balanced against the need to counter genuine risks of societal harms, we do assert that there can be a 'chilling effect' felt for rights to freedom of expression should regulation of the collection and use of personal data by the police be, in fact or in perception, too lax, affecting as it does trust in those tasked by the state to protect the public [31]. We have no wish however to fall into the trap of giving credence to either the 'nothing to hide, nothing to fear' or 'Big Brother' arguments, nor to those who argue that security versus privacy is an 'all-or-nothing' situation. [32] In addition, care must be taken not to contribute to the polarisation of the debate, to use, as Anderson put it, 'opposing caricatures of unprecedented threat and snoopers' charter'[33] or to let one's own personal attitudes to state bodies, whether this be one of trust, fear, contempt, admiration, suspicion or otherwise, to overly cloud the review. The authors themselves hold differing personal views on whether the Supreme Court decision in *Catt* was the 'right' one.

Supranational regulation of police databases is also explored in this piece, by way of the examination of some recent pieces of case law from the European Court of Human Rights and European Court of Justice, as is recent national-level guidance applicable in the UK in relation to the retention and possible deletion of police database records. However, there is not space in this piece to consider every nuance of the developments which contemporarily give great fluidity to UK surveillance and security law. There has been a recent series of interlocking and increasingly blurred doctrinal developments that touch upon the area of police intelligence regulation, and we have chosen to examine *Catt* as a doctrinal development most squarely, in the knowledge that other authors from our field will be addressing in turn issues such as the 'ripple effect' at domestic level that has come from the impact of the decision of the European Court of Justice in the *Digital Rights Ireland* case (where the ECJ determined that the EU Data Retention Directive

was disproportionate in allowing too unrestricted a level of access by state agencies to telecommunications and internet records held by service providers) [34].

In the latest 'ripple' to arrive on our shores, the High Court of England and Wales in *Davis* has deemed part of the UK government's response to the decision in *Digital Rights Ireland* to be unlawful [35]. This response was in effect the emergency enactment by Parliament of Section 1 of the Data Retention and Investigatory Powers Act 2014. Section 1 of the 2014 Act has been disapplied, although under an order delayed until April 2016, due to the lack of safeguards around state access to private records held by 'communications service providers', (the Court basing its decision on the criteria set out in *Digital Rights Ireland*), and, significantly, furthermore because of the extent of the protection to personal data afforded under the EU Charter of Fundamental Rights. The Charter was deemed justiciable in the case of *Davis* because of other, bigger 'ripples' in recent UK public law developments [36]. This disapplication of a provision in the UK surveillance law framework using the Charter is a truly novel and significant development, which has constitutional repercussions which we do not have room to explore in detail. Suffice to say that the intrusion of EU data privacy law into the traditional state security purview of central government may have serious implications in a time of debate over 'Brexit' [37] and wider human rights law reform[38]. In a similar vein, we do not have room to fully acknowledge the potential implications or substantive content of the draft EU Police and Criminal Justice Data Protection Directive, or indeed the great upheaval that might be caused by a new forthcoming EU Data Protection Regulation, but with regard to the recent decision in *Davis* we can at least, below, draw some thematic and domestic legal parallels with the issues in *Catt* in the Supreme Court.

Despite these fluidities in the relevant doctrinal framework, which we feel were necessary to acknowledge, in the last Part of this piece some conclusions will be drawn and some recommendations and wider observations made as to how, as a feature of broader police accountability in the UK, we feel it may be that police databases could be more closely and effectively regulated over time. However, the next Part of this piece considers the range and operation of a number of different police intelligence and 'criminal records' databases in the UK context, to give a more detailed grounding for our later, primarily legal analysis.

4. THE POLICE USE OF DATABASES IN THE UK CONTEXT

In contemporary political and legal dialogue, there is a great focus on issues of state surveillance; and principally covert, electronic and 'mass' surveillance at that[39]. But police records from 'intelligence' databases of different kinds warrant the same or arguably more rigorous scrutiny - populated as they are with the sensitive personal data of those people who come into contact with the police, as part of the criminal justice system, in different manners - from suspects, associates and those on the periphery of suspicious activities, those charged with offences, convicted offenders, and those acquitted of offences; to witnesses, victims, and the police themselves. From a classic civil liberties perspective, protagonists in the most sensitive of these police intelligence records might be seen by the *state* as 'challenging' individuals, and as part of 'worrisome' groups, ranging from protestors and demonstrators, through a range of notions of extremists, from those of peripheral interest up to and including those representing the most concrete risk to society such as terrorists and those who would incite terrorism. Other databases in turn will encompass records relating to the most 'risky' people in UK society from the perspective of the protection of the public from violent and sexual harms [40].

In the specific context of the United Kingdom, police and other criminal justice databases have increased in importance as a mode of facilitating intelligence-led policing, and include "the Police National Database [PND], the Violent and Sexual Offenders Register (known as ViSOR'), the (central) National Offender Management Information System (NOMIS or C-NOMIS), the Electronic Offender Assessment System (E-OASys), the much-critiqued National DNA Database (NDNAD), local police databases on interactions with offenders, victims and witnesses to crimes, as well as the particular databases held and operated by specialist units of the Metropolitan Police and so forth, such as the National Domestic Extremism and Disorder Intelligence Unit database of overt and covert surveillance records." [41]

The Police National Database or 'PND' (formerly the Police National Computer, or 'PNC') is in effect exactly what it says it is: a database that can be accessed, amended and added to by all regional police authorities including in Scotland and Northern Ireland and by some partner agencies, in particular circumstances, on a nationwide basis. As such, the PND is a key component in the facilitation of intelligence-led policing, and indeed, could be seen as the largest repository of 'police intelligence'. However, the issue of the appropriate regulation of police databases in many ways turns on what may be lawfully gathered and included, as well as then shared, from this database. This database includes information which has been categorised as 'criminality information'. 'Criminality information':

"… can be broadly defined to include categories such as allegations, records of arrest and/or charge and/or prosecution, statements by witnesses and (alleged) offenders themselves, cautions, convictions, records of penalty notices for disorder, sentencing reports, tax and/or benefit investigations, the placement of individuals on barring lists, and covert or overt police surveillance intelligence-as well as more peripheral 'intelligence' such as anti-social behaviour orders and reports of anti-social behaviour itself (despite the seemingly non-criminal nature of this behaviour by its very definition)." [42]

In relation to the population of police databases, one of the first steps that should be taken by the police when evaluating information is to separate information from intelligence, and then to categorise intelligence in terms of type of information and level of risk. [43] For instance, 'Group 1' information on the PNC/PND contains information about an individual that centres on the need for public protection. HMIC found however that there were inconsistences between police forces in the use of, and the rules surrounding, these categorisations and also inconsistences in the uploading of information to the Police National Database, with two forces failing to upload core intelligence records. [44] As the Police National Database is an analytical database, not one which provides an instant check or automatic linking to other

records, these inconsistencies between police forces could have serious consequences for the police's ability to make valuable links for the purposes of crime prevention and detection. In addition, the Independent Surveillance Review noted that there did not appear to be a common view on the most appropriate length of time for retention of data; it may vary per agency or by type of data, or by type of crime, [45] with some forces attempting automated record deletion processes without a manual intervention. Add to this our earlier points about the lack of clarity between 'intelligence' and 'intelligence products' we may start to wonder also about the process of production of such 'products'. The APP acknowledges that drawing inferences from analysis requires objective thought and may suffer from 'cognitive bias'. [46] However, as we explore later in this piece, there are developing judicial lines of thinking that suggest a criteria-based approach to intelligence retention might be required - an acknowledgment by the judiciary, perhaps, that police intelligence retention cannot be hyper-regulated in any meaningful way, even though the law requires the base level of standardisation and certainty that a principles-based approach would offer [47]. Indeed, the field of medical and patient information governance has recently been undergoing its own period of self-study and reflection in relation to the future adoption of principle-based approaches to (personal) data retention and sharing [48].

The core issue for this piece is the retention (and, implicitly, the use) of police intelligence, within police databases. Some of these databases are created or designed to facilitate the policing of particularly 'risky' or dangerous groups or individuals in society. As such, there is a general understanding that the more comprehensive their reach, and the more detailed and nuanced their historical record in relation to dangerous individuals, the more effective a tool they will be in the policing, for example, of 'domestic extremism', or sexual offending [49]. The permanent removal of information about individuals is in essence something that can be viewed as the reduction in the level of information about risk - and in the context, too, that some of these are risky individuals indeed. It has argued been that:

"those tasked with the protection of the vulnerable may well be concerned that premature deletion, or suppression, of intelligence will hamper their ability to use information to make connections. It is therefore vital that a well-reasoned and evidence-backed justification for every stage of personal data processing -- collection, retention and disclosure -- is made out and recorded." [50]

For example, the national police database known as the Violent and Sexual Offenders Register, or 'ViSOR', has a considerable public protection function, as a grouped set of data about individuals who are known to be great risks to public safety. But perhaps because of its core public protection function, and lack of any distinct biometric functionality, ViSOR has never been subject to much commentary or campaigning by privacy advocates, comparatively speaking. On the other hand, the National DNA Database has been the subject of considerable legal scrutiny, statutory reform, and academic critique.[51] [52] A smaller and less well-known but commensurately specialised database is that known (in the recent *Catt* judgment in particular) as the Domestic Extremism Database. This database was the direct object of the challenge in *Catt* [53]. Local police databases operated by particular police forces also abound [54].

Information about individuals can be inserted into police databases in an array of different media and formats - text, of course, but also photographs of individuals, as well as video, can feature on police databases as a way of identifying individuals or linking them to particular incidents or offences[55]. Photos and videos, as biometric information, raise concerns more readily because of the perceived sensitivity of their very nature as particularly identifying or 'personal' items of police intelligence; as well as the manner in which such material can underpin the function of more privacy-infringing technologies. The House of Commons Science and Technology Committee, for example, have had recent cause to observe that they were:

" particularly concerned to hear that the police are uploading photographs taken in custody, including images of people not subsequently charged with, or convicted of, a crime, to the Police National Database and applying facial recognition software. Although the High Court ruled in 2012 that existing policy concerning the retention of custody photograph by the police was "unlawful", this gap in the legislation has persisted." [56]

Indeed, the recent news that Police Scotland have been practising this method of compiling and analysing individual photographs for crime detection has raised considerable consternation in the press[57]. While in *JR38* it was held by a majority of the Supreme Court that teenagers engaged in sectarian public disorder did not have a reasonable expectation of privacy (and so Article 8 ECHR was not engaged), and so it was lawful to attempt to identify them through the publication of surveillance images in an appeal via a local newspaper, this was a decision that was influenced heavily by the reasoning around the nature of the disorder they were engaged in (a criminal series of acts involving throwing stones at police officers, and so forth) as well as notions of their best interests as children (who should be sought out and dissuaded from pursuing a career in violent sectarianism). Cases prior to *JR38*, such as *Wood* in the Court of Appeal, discussed below, suggest that there is something particularly intrusive about photo and video surveillance, and the use of that material in police intelligence processes, and so this intelligence imagery is more likely than text-based records to engage Article 8.

In the case of *R (Wood) v Commissioner of Police of the Metropolis* [2009] EWCA Civ 414, the claimant, an anti-arms trade campaigner, was photographed by the police when leaving a corporate meeting, which he had attended as a shareholder of the company connected to the arms trade; having attended to publically voice his dissent against the corporate practices he stood against. This image of him was retained for broad intelligence purposes, in essence for his future identification at anti-arms trade campaign events. The retention by the police of this photograph, even when not placed in an intelligence database, was deemed by the Court of Appeal to be an unjustified interference with the claimant's right to respect for private life under Article 8 of the European Convention on Human Rights. Essentially, the Court of Appeal determined that when it was established that Wood had committed no criminal offences during or in the area surrounding the shareholders' meeting, images taken of him for identification purposes should have been deleted, not retained indefinitely. *Wood* was not addressed in any great detail in *Catt* in the Supreme Court. In the two cases information about the claimants was gathered in broadly the same manner, in

public, and in circumstances where each claimant might be expected to have the requisite 'reasonable expectation of privacy' in order that their Article 8 rights were engaged (they were both personally non-violent). John Catt however failed in his attempt to have *written* entries on a police intelligence database deleted. It is arguable that there is now a difference in the courts' treatment of written police intelligence information on the one hand, and image based intelligence on the other, emerging following the Supreme Court decision in *Catt*, although it should be noted that the context of Mr Catt's association with individuals who had engaged in serious violence seemed to have been a significant factor. It appears unclear as to whether the underlying deciding factor in these decisions is the type of information retained, the circumstances of its collection or the context in which it is held. [58] This is undesirable in terms of the foreseeability of the law and guidance for police decision-makers and may go some way to explain the current lack of consistency across police forces regarding the retention of custody photographs.

The brief overview provided in Part 4 of a few cases, above, and particularly *Wood*, show that the use by police of personal data, or information with an intelligence value, can be highly varied in nature, and certainly varied in terms of the format in which it exists. It is now appropriate to turn to the issue of the legalities of the *retention* of police intelligence material on databases, versus the issue of the *sharing* of that intelligence for public protection and other operational purposes, in more detail.

5. POLICE INTELLIGENCE RETENTION AND REGULATION AS A HUMAN RIGHTS ISSUE

There are key distinctions to be made between retaining, and on the other hand the sharing or disclosing of 'police intelligence' or 'criminality information'. The combined effect of the recent decisions in *Catt* and *JR38* in the Supreme Court has now created what we understand to be the following position in the resulting common law on police powers: that retaining personal information as intelligence, for example, on police databases at least engages the qualified right to respect for private life under Article 8 of the European Convention on Human Rights ('Article 8 ECHR')[59]. If Article 8 can be said to be *engaged* by the retention of intelligence on police databases, it is also the case that the lawfulness or requisite proportionality of the retention of the relevant information depends to some extent on the format and nature of the information concerned, (with the length of the retention of photographs and videos being more closely scrutinised by the courts), the nature of the activity engaged in by the individual or their associates, the circumstances of its collection and how easily the information can be searched for, retrieved and linked to intelligence identifying others. This is shown by the distinguishing factual features of *Wood* in the Court of Appeal, where a specialised database had been created to hold images of protestors gained through police surveillance, as compared to *Catt* in the Supreme Court, where Catt had had his personal-indexing, text-based 'nominal' records deleted, but was still identified as present in the records of certain demonstrations.

When it comes to issues of the sharing or dissemination of police intelligence for crime prevention or public protection purposes, so long as the 'reasonable expectation of privacy' is not removed or absent, as it would be for a person more clearly and certainly engaged in public disorder or other crime (the case in *JR38*), then Article 8 ECHR is likely to be engaged.

As has been observed however, an argument can be made that there should be "a distinction …, from an Article 8 perspective, between long-term retention of personal data, and the disclosure of that data. In addition, individual pieces of intelligence are inherently partial and often unreliable, in the sense of being unverifiable. But should unreliability, of itself, mean that a piece of intelligence should not be retained or shared where appropriate?"[60] Indeed, the police in the UK recognise that the reliability and certainty of intelligence should be recorded (in the "5x5x5" National Intelligence Model format) so that future use of that information can benefit from this context [61]. This model does set down a number of criteria by which intelligence is assessed for current and future reference purposes, in some way reflecting the criteria set down by Behrens J in the case of *R (SD) v Chief Constable of North Yorkshire* [2015] EWHC 2085 (Admin) for the sharing or public protection disclosure of intelligence in the form of criminality information. These criteria, first explored in a systematic way by Neuberger LJ in the Supreme Court case of *R (L) v Commissioner of Police for the Metropolis* [2010] 1 A C 410, require disclosure decisions to be made on the basis of the *reliability* of the information, the *gravity* of the matter, the *relevance* of the information to the risk to be managed, the lapse of *time* between the originating event the information describes and the present day, the *impact* of the disclosure on the subject, and the overall *proportionality* of the possible disclosure.

There are multiple statutory and common law avenues through which criminality information sharing might take place. Figure 1, below, is a table which gives a sense of the variety of manners in which this criminality information sharing ('CIS') takes place, and their underpinning legal bases.

Fig. 1: Crime prevention strategies, CIS and legal bases	Domestic Violence Disclosure Scheme (DVDS)	Multi-Agency Public Protection Arrangements (MAPPAs)	Child Sex Offender Disclosure Scheme (CSODS)	(Enhanced) Criminal Record Certificates (ECRCs)	'*Riaz* orders': identifiable inherent jurisdiction injunctions	Local authority and police Pubwatch schemes
Operational contexts and the role of the particular method of CIS	*Domestic violence - 'Clare's Law'; The Scheme allows for the*	*Serious violent and sexual offending - 'Safeguarding' and 'public*	*Sexual offending against children - 'Sarah's Law'; individuals*	*Employment vetting in higher-risk settings - where certain specified*	*The prevention of 'child sexual exploitation' (CSE) in the public naming*	*Preventing violence in the night-time economy by sharing the*

as a crime prevention strategy, of a certain type	*disclosure to those at risk of harm of information relating to domestic violence, though not any information relating to spent convictions.*	*protection'; disclosures of information to those at risk of sexual or violent harms, or responsible for those who might be at risk themselves.*	*responsible for children can request the police disclosure to them the offending history of an individual they feel is a risk to a child*	*occupations are exempted from the provisions of the Rehabilitation of Offenders Act 1974, and employers can require an ECRC.*	*of individuals subject to an injunction preventing them from contacting children not already known to them prior to the order.*	*images and personal details of violent individuals banned from one licensed premises amongst other premises in order to bar them from those.*
The legal bases for the avenue of CIS concerned	Police common law powers to disclose information.	Police common law powers to disclose information.	S.327A of the Criminal Justice Act 2003 (as amended).	S.113B of the Police Act 1997 (as amended).	The 'inherent jurisdiction' of the High Court.	Private law relationship between licensees and public.
Responsible public bodies and particular 'user' agencies and individuals	Police, social work, education, health and probation professionals working in a local multi-agency forum.	Police, social work, probation and other professionals working according to statutory offender monitoring processes.	Police, social work, education, health and probation professionals working in a local multi-agency forum.	Employers in relevant areas; and the police, working with the Disclosure and Barring Service (DBS).	Local authorities and the police in a given force area will now be able to apply for these particular '*Riaz* orders' to fight CSE.	'Crime reduction partnerships' between local authorities, pub/club licensees and the local police.
Notes on relevant case law developments	As yet, not dealt with specifically by the courts in any particular litigation. *R v Chief Constable of North Wales Police and Others (ex parte Thorpe and Another)* [1999] QB 396 establish a 'pressing need' test for disclosure, on a proportionate and necessary basis.	*R (XX) v Home Secretary* [2014] EWHC 4106 (Admin) established that MAPPA Guidance which allows for disclosures on the basis of police common law powers to share information to protect the public is 'in accordance with the law' with regard to Article 8 ECHR.	Following *R (X) v Home Secretary* [2012] EWHC 2954 (Admin) greater emphasis has been placed on the procedural rights of sexual and violent offenders to be consulted before disclosures are made in MAPPA or CSODS regimes using common law powers.	*R (T) v Chief Constable of Greater Manchester* [2014] UKSC 35 found ECRCs incompatible with Art 8 ECHR, since they allowed indefinite scope for disclosure re trivial items of criminality information; though there was resulting reform.	*Birmingham City Council v Riaz and others* [2014] EWHC 4247 (Fam) saw the High Court move to recognise that criminal prosecutions are difficult to mount successfully in some CSE cases, and so the civil standard of proof can be used to apply the sanction of an identifying injunction etc.	*R (Proud) v Buckingham Pubwatch Scheme* [2008] EWHC 2224 (Admin) and *R (Boyle) v Haverhill Pub Watch* [2009] EWHC 2441 (Admin) both establish that Pubwatch schemes are not amenable to judicial review, despite police involvement.

Much of the doctrinal development in this area of Article 8 ECHR case law that is concerned with 'criminality information sharing' has stemmed from a body of litigation around the issuing by the police (in partnership with the Disclosure and Barring Service) of 'Enhanced Criminal Record Certificates' (ECRCs), which are required by employers where there are public protection dimensions to employment . This litigation has effectively 'peaked' in doctrinal terms in the form of the Supreme Court decision in *R (T and another) v Home Secretary and another* [2014] UKSC 35. Appropriate 'filtering' rules for the contents of ECRCs, used in large swathes of employment sectors, including education, health, social care, criminal justice, and so on, were deemed to be essentially non-existent in the same case in the Court of Appeal in 2013. This Court of Appeal judgment then led to reforms in the ECRC system through a series of Orders laid before Parliament in the summer of 2013. The declaration by the Court of Appeal that the ECRC filtering rules then in place were incompatible with Article 8 of the European Convention on Human Rights was upheld in the Supreme Court judgment itself. The reforms to ECRC filtering rules themselves, however, have been (unsuccessfully) challenged as being 'light touch'; merely precluding a single, first conviction or caution for some less violent offences from being shared, and as long as a sufficient period of time has passed [62]. As was noted by Simon J (at para. 65) in this recent unsuccessful challenge in *R (W) v Secretary of State for Justice* [2015] EWHC 1952 (Admin), it was necessary to recognise "that almost any system which could be devised may lead to harsh results at the margins". Of course, in systematising any decision making process with rules, rather than more elastic criteria, there is always a risk of overly reducing discretion (in ECRCs, of the police to take into account the circumstances surrounding the relevant conviction).

It is fair to say that there is more guidance regarding the sharing of criminality information, however complex, than there is for intelligence retention. It was hoped that the Supreme Court decision in *Catt* would have provided more clarity and so we now turn to the doctrinal issues in this case.

6. THE RECENT SUPREME COURT DECISION IN *CATT*

The recent Supreme Court decision in *Catt*[63] has shown a move toward greater recognition for the realities of policing based on 'intelligence', whether of a value from relatively low to very high. But it is possible to have a range of views as to the future impact of this decision to deem lawful the retention of scraps of intelligence about one peaceful or non-violent protestor as part of the 'jigsaw' of intelligence on the more violent group with which they associate.

Some basic factual points to note about the case, now that we are offering up a more detailed critique of the judgment in this Part of our piece, are that Catt has no criminal convictions, is 92 years old, and has never been violent *personally* at anti-arms trade rallies or other political demonstrations (although groups with which he associated had engaged in violence). Catt has been arrested, but not charged, on two separate occasions at protests, for the offence of obstructing a highway. Records on police databases recorded his presence at protest events, his appearance, demeanour and peaceful protests activities (including sketching police and protestors on a notepad etc.). Catt had already achieved, through the use of subject access requests under the Data Protection Act 1998, an idea of the scope of the records that were held about him and his protest activities and associations, and had already convinced the Metropolitan Police authorities that the disparate pieces of information concerning him should no longer be connected with the use of a 'nominal profile' - an index entry, in effect, which marks an individual of note to investigators of criminality, here in the public protest context. What remains are mentions of John Catt in the reports and intelligence describing other activists and demonstrators at particular events and protests which he attended. The Supreme Court noted in its judgment that extensive weeding of 'nominals' had gone on over a period of time in order that this indexing of individuals was proportionate. It accepted the police's argument that to undertake the wholesale weeding-out of the residual component records of those whose nominal profiles were removed would result in an enormous, potentially unworkable, administrative burden - but that argument as to costs and resources was not significantly entered into, since the Supreme Court determined that the retention of those more fragmentary intelligence records concerning John Catt could be justifiably retained, given his links as a member of various groups to the more violent and radical activities of others. Importantly, the Supreme Court decision in *Catt* means that these fragmented intelligence records need not be automatically deleted as they form part of a 'jigsaw' of intelligence on the protests.

Giving up part of that intelligence 'jigsaw' in the context of policing public disorder, domestic extremism and other public protection risks is an anxious exercise for the state. Tellingly, given the wider context of the impact the outcome of *Catt* will or would have, it has been written that:

" For anyone whose job it is to protect others from harm, one of the most difficult tasks is to decide when to delete personal information. Personal data collection by the public sector, and the sharing of those data, is often subject to criticism in the media, and to the risk of close scrutiny in the courts. Yet taking a decision to delete can never be an exact science, and there is often an underlying fear that a deleted piece of information might turn out to be the missing link that would have identified a risk to another person." [64]

There are a number of particular competing policy issues in the domain of retaining information on police databases, which are highlighted by *Catt.* The first such policy concern is the notion that individuals should be as free from state intrusion and monitoring as the necessary requirements of public protection will permit - the classic civil libertarian perspective - and that the state should be able to forget misdemeanours, as well as forgive them, in the aim (particularly in this case) of avoiding the chilling of public protest in a democratic system with a tradition of the same. In *Catt* in the Court of Appeal, where John Catt was successful, Moore-Bick LJ noted, for example, that "Even information of a public nature, such as a conviction, may become private over the course of time as memories fade, thereby enabling people to put their past behind them …" [65]

However, there do exist in UK society a range of groups who present a public protection risk - and there is the argument, reflected in the eventual outcome of John Catt's case, that there are those individuals, who, even as peaceable 'hangers-on' in more radical, even violent, circles, must forgo a better protection of their personal 'informational privacy' or 'right to informational self-determination'. In *Catt* in the Supreme Court, Lord Sumption (at para. 31) [emphases added] argues that:

"The composition, organisation and leadership of protest groups who are persistently associated with violence and criminality at public demonstrations is a matter of proper interest to the police even if some of the individuals in question are not themselves involved in any criminality. *The longer-term consequences of restricting the availability of this resource to the police would potentially be very serious. It would adversely affect police operations directed against far less benign spirits than Mr Catt. Organised crime, terrorism, drug distribution and football hooliganism are all obvious examples.* One cannot look at an issue of this kind simply in relation to Mr Catt."

There was a particular kind of sub-narrative which developed in the *Catt* judgment in the Supreme Court which had not surfaced to the same extent in earlier iterations of the case. There was a sense, as a kind of classic 'floodgates' concern, that if John Catt were to succeed in the face of public policy arguments for the retention of his data within police intelligence databases, and have those records then deleted, then this might lead to a situation where intelligence retention in very sensitive areas of UK policing might be fatally compromised. Chief amongst these issues as raised in the Supreme Court judgment in *Catt* was the idea of intelligence gathering and retention in relation to the histories and 'criminality information' of domestic violence perpetrators.

As Lord Sumption has in *obiter dicta* in *Catt* (at para. 43):

"[Particular] kinds of offence are often characterised by the development of abusive behaviour over a long period of time. This is especially true of domestic violence, a difficult and sensitive area in which the protection of persons at risk may require sensitive monitoring over a considerable period."

Similarly, and perhaps more passionately, Lady Hale (at para. 54) commented that:

"It is well known that, for a variety of reasons, complaints of domestic violence are often not followed through to prosecution and conviction. But it is vital for the police, when responding to any new complaint, to know whether there have been similar complaints in the past. Domestic violence often escalates in seriousness with each new incident, and the police have to be aware of this when considering how to respond. It is not too dramatic to say that lives have been saved as a result."

In the same decision again, once more in *obiter*, Lord Toulson (at para. 76) also concluded that, in relation to the retention of the types of criminality information reaching the lower thresholds of certainty only (such as complaints or allegations, as opposed to convictions, with the latter having reached the standard of proof of guilt 'beyond reasonable doubt', for example):

"The response of the police to complaints about abusive conduct may well be affected by knowing whether similar earlier complaints have been made against the same person, either by the same or by other complainants. In those circumstances I do not consider it to be unlawful for the police to adopt a standard practice of retaining a record of such complaints for several years, but with a readiness to be flexible in the application of the practice."

So the judgment by the Supreme Court in *Catt*, in many ways, was not just about, and does not touch upon the regulation of a single police database, in relation to the intelligence records describing just one individual of little risk to society: instead, the decision in *Catt* could be seen in the minds of the Supreme Court justices in the relevant panel to have distinct ramifications for the policing of harmful behaviours across society as a whole. In this regard, the Supreme Court could be seen to be reflecting current policing concerns regarding the importance of effective data retention and sharing. In its *Building the Picture* report, HMIC commented on the importance of consistent data sharing in observing crucially, from a policy perspective, that:

"In the light of case law and high-profile cases such as Jimmy Savile's long period of sex offending, we are materially concerned about the extent to which the police service is responding fully to the responsibilities inherent in a changing environment, where speedy access to up-to-date and relevant information is essential. For example, we found cases where forces had not revisited their position since the whole of the police service completed local information management implementation plans in 2010. In this regard, the absence of appropriate audit and assurance regimes (to check that information is being appropriately assessed, retained or disposed of) is especially worrying, and needs to be addressed swiftly." [66]

However, while the relevant lines of jurisprudence and regulatory policy might be converging post-*Catt* to at least some extent, it is not so clear that our own recent case law, and particularly the outcome in *Catt*, is consistent with the European view of similar police operational intelligence issues. If we consider the manner in which the European Court of Human Rights, with its quasi-supervisory jurisdiction over the UK Supreme Court, has come to determine some of its own views on police intelligence and criminality information retention, in relation to one particular case at least, we can see a marked difference emerging in comparison with contemporaneous UK jurisprudence. The Registrar of the European Court of Human Rights has observed (at least in a press release), that in *Brunet v France* (2014) (application no. 21010/10), a case concerned with the potential deletion of (and refusal to delete) an allegation of domestic violence from a police intelligence database, it was the case:

"that the information contained in the database was quite intrusive in nature. While that information did not contain the individuals' fingerprints or DNA profile, it consisted of details on identity and personality, in a database that was supposed to be used for researching crimes. In addition, the retention time of the personal record, 20 years, was particularly lengthy in view of the fact that Mr Brunet had not been found guilty by a court and that the proceedings had been discontinued… the Court took the view that the State had overstepped its margin of appreciation in such matters, and that the rules for the conservation of records in the STIC database, as applied to Mr Brunet, did not strike a fair balance between the competing public and private interests at stake. Accordingly, the impugned retention could be regarded as a disproportionate interference with Mr Brunet's right to respect for his private life and was not necessary in a democratic society." [67]

The difference with the outcome in *Catt* is marked. The UK jurisprudence, in the form of *Catt* at least, treats domestic violence perpetrators and groups of protestors, violent or otherwise, exactly alike for the sake of the 'jigsaw' argument of operational necessity; while the European Court of Human Rights, perhaps, might prefer to distinguish the risk posed individually by a non-violent protestor such as John Catt from the societal risk posed by an alleged domestic violence perpetrator. We shall see if John Catt is granted permission to proceed to a hearing by the Strasbourg Court. To date, however, little has been written about the decision in *Brunet v France*, since:

"Sadly, the judgment in *Brunet*, which is in French, does not give a detailed explanation of the French retention scheme. It is therefore difficult to make precise comparisons between the French and domestic schemes. However, it would seem that [UK regulation of police intelligence] may be open to challenge on the basis of this judgment." [68]

The doctrine of the margin of appreciation might support the UK government if *Catt* case were to be re-examined at the level of the Strasbourg court. It is possible to make comparisons with the facts of *Brunet* and the situation in *Catt* but the common law basis of much public order policing in the UK, including powers to gather and to use police intelligence might mean that in the UK, police intelligence retention in the public order policing context of *Catt* might be readily deemed justifiable by the European Court of Human Rights through applying the margin of appreciation. It is interesting, though, to note that the *Brunet* decision was given only minimal consideration in the Supreme Court judgment in *Catt*.

UK case law is already moving on in a way, post-*Catt*, that might yet see considerable shifts in the regulation of police intelligence, if not precisely on the same point as in *Catt* (that is, on the retention of intelligence about relatively peaceful protestors). We commented upon the recent case of *Davis*[69] in section 3 above. Although the Court ultimately disapplied section 1 of the 2014 Act, for Bean LJ the European Court decision in *Digital Rights Ireland* must be interpreted to mean that (para. 95) 'a wholly innocent person's data might be accessed in order to assist in the detection of serious crime by others. The need for access to data is not limited to data directly attributable to particular individuals suspected of having committed serious crimes'. This would seem to reflect strongly the views of the Supreme Court in *Catt* on the nature of intelligence and data-led policing. The Court however went on to determine that (at para. 98), as per the European Court of Justice decision, access to communication data retained in bulk by communications service providers requires 'independent approval.' This kind of independent judicial oversight is not required for decisions to collect and retain police intelligence at the moment.

7. A BROADER COMMENTARY AND CRITIQUE OF THE SUPREME COURT DECISION IN *CATT*

A commentary, or a critique, of the Supreme Court decision in *Catt* is ultimately a commentary or critique of the judgment of Lord Sumption in the case - it is the first of the judgments, the lengthiest, and the most uncompromising in tone. Lord Sumption addresses directly the issue of Article 8 ECHR engagement in the case, and the notion of Article 8 as a qualified right, by observing (at para. 6) that: "it is clear that the state's systematic collection and storage in retrievable form even of public information about an individual is an interference with private life… It follows that the present appeals turn on article 8(2) of the Convention, and in particular on whether the retention of the data is (i) "in accordance with law", and (ii) proportionate to its objective of securing public safety or preventing disorder or crime."

However, for Lord Sumption in *Catt* (at para. 12), in his judgment, the quality of a lawful interference with qualified rights being 'in accordance with the law' "does not mean that the law has to codify the answers to every possible issue which may arise. It is enough that it lays down principles which are capable of being predictably applied to any situation." Lord Sumption seems to have in mind the notion that the indefinite retention of police intelligence, or nearly all police intelligence, is what is being challenged, and that the case was one to use to determine principles applicable to the retention of data about any group or individual by the police - where that person or group is a public protection risk - rather than set thresholds for the deletion of data or intelligence where a certain (low) profile of risk is presented on the facts.

Interestingly, Lord Sumption deployed a four-part, or 'quadripartite', test as to the proportionality of an interference with rights in his judgment in the Supreme Court in the case of *R (Bank Mellat) No.2 v HM Treasury* [2013] UKSC 39, stating that a measure of the proportionality of an interference with ECHR rights required:

" exacting analysis of the factual case advanced in defence of the measure, in order 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."

While, as David Hart QC has observed, Lord Reed in *Bank Mellat* constructed a four-part proportionality test that is less vague than the proportionality standard applied by the Strasbourg court, the Strasbourg court cannot apply as nuanced a proportionality analysis as a national court can do, since the Strasbourg court must recognise more explicitly the nature of the domestic, national 'margin of appreciation'[70]. Lord Sumption in *Bank Mellat*, in accordance with this more granular, domestic approach that can be favoured by the Supreme Court, deployed the above 'quadripartite' test in his judgment, saying that the proportionality test could be 'sufficiently summarised' in that way. However, this quadripartite proportionality test is absent from the text of Lord Sumption's judgment in *Catt*. In *Catt* (at para. 17), Lord Sumption noted that:

"In my opinion, the retention of data in police information systems in the United Kingdom is in accordance with law. The real question on these appeals is whether the interference with the respondents' article 8 rights was proportionate to the objective of maintaining public order and preventing or detecting crime. For this purpose, it is necessary to look separately at the two cases [that of Catt, and that of T] before us, for the relevant considerations are very different."

However, in *Catt*, when considering the proportionality of the interference with the Article 8 ECHR rights of both Catt and T, Lord Sumption did not expressly apply the four-part test he deployed in *Bank Mellat*. The approach Lord Sumption (and other Supreme Court justices in the panel for the case) seems to have taken is that the challenge in *Catt* was to the police intelligence system of retaining pertinent information of various kinds, about individuals, and therefore about 'risky' *groups*, in the 'jigsaw' concept outlined above. We do not see whether Lord Sumption has considered that a less serious, or more minimal interference in the rights of an *individual* like John Catt (as per the third part of the quadripartite proportionality test) would include the systematic review and deletion of his records over time, however costly, where a person has demanded it. In essence, there is no substantive consideration of the idea of a 'more minimal interference' principle in the case to the detriment of the rights of those in the same situation as John Catt in the foreseeable future. The principle of the overarching necessity of the 'jigsaw' is established, to the benefit of operational, intelligence-led policing, particularly in relation to public order circumstances and risks.

Tellingly, there is also no specific consideration in the entire *Catt* judgment as to whether the retention of the data in Catt's case, or T's case, as individual matters, was something that addressed a 'pressing social need' - the test regularly and routinely used by the European Court of Human Rights to determine if the interference with the qualified right in Article 8 was 'necessary in a democratic society' (and thus part-way to being deemed lawful, in alliance with tests for 'legitimacy' and 'proportionality'). Lady Hale does admittedly highlight that in her view, the crucial factor is as much whether the retention of information was 'necessary in a democratic society' as whether it was proportionate retention [49]. Lord Toulson also considers the issue of the necessity of

retaining information about John Catt in the relevant database; and, however, finds the required necessity lacking, and would have seen Catt's case (though not T's) succeed [65] [71]. Perhaps if *Catt* were to appear at Strasbourg, the discussion would turn more on whether the retention of police intelligence concerning an individual, such as Catt, who presented such little risk of violence as a demonstrator, really did constitute, as an interference with the Article 8 ECHR right to respect for private life, a response to a 'pressing social need' to monitor and place under ongoing surveillance those who presented a risk of public disorder or serious harm.

However, as noted above, Lord Sumption deploys the test for 'legitimacy' ('in accordance with the law') but not a test for proportionality of his own devising - or anyone else's. Since the relevant test for 'necessity', at least in the form of a 'pressing social need' is also not deployed in his judgment, it is difficult not to turn, questioningly, to the traces of policy and those ideological stances relied upon by Lord Sumption in justifying his dismissal, ultimately, of both of the cases brought by Catt and T alike.

Perhaps the outcome in *Catt* would have been different if the case was about a nominal record, rather than a passing reference to an individual in a database; since Lord Sumption implies that an unlinked record is not as particularly intrusive as an 'indexing' or 'linking' record that provides greater 'searchability'. But this seeming nuance of database operation and design does not take into account the true, current functionalities or potential future functionalities of database technologies; whereby (assuming steps are taken to consolidate the variety of records management systems used by police forces) all and any scraps of police intelligence will be summoned as easily as those currently linked by PNC/PND 'nominal records', or even more so.

Lord Sumption's policy stance seems to be that the mere inclusion (even the indefinite inclusion) on a police intelligence database, is, ultimately, nothing to be concerned about, or nothing to be complained about. To quote him at length, he writes (in *Catt* at para. 27) that:

"The retention in a nominal record about a particular person or in an Information Report about a demonstration of information about other persons such as Mr Catt who were participating in the same event does not carry any stigma of suspicion or guilt. Mr Catt takes exception to what he regards as the inference that all those mentioned as participating in events such as Smash EDO protests are "extremists". But that is not a fair inference. The relevant police units are concerned with "extremism", in the sense of the pursuit of a political cause by criminal means, but it does not follow that all those who are recorded as attending these events are being characterised as extremists in that or any other sense. Unlike the records of criminal convictions or cautions, the information would not be regarded as discreditable to those who were merely recorded as attending an event at which they were not alleged to have committed offences. But in fact, the material is not usable or disclosable for any purpose other than police purposes, except as a result of an access request by the subject under the Data Protection Act. It is not used for political purposes or for any kind of victimisation of dissidents. It is not available to potential employers or other outside interests. There are robust procedures for ensuring that these restrictions are observed. Finally, the material is periodically reviewed for retention or deletion according to rational and proportionate criteria based on an assessment of danger to the public and value for policing purposes."

There are two key points to make about this long passage quoted here. Firstly, when he writes that 'unlike the records of criminal convictions or cautions, the information would not be regarded as discreditable to those who were merely recorded as attending an event at which they were not alleged to have committed offences ', Lord Sumption does appear to be treating 'intelligence' differently and regarding it as less intrusive, at least in Mr Catt's case, than criminality information as we would define it, taxonomically. We might assume that, in Lord Sumption's view, Mr Catt was hardly on the radar, let alone under the microscope. Secondly, there is an assumption here about the subjective feeling experienced by those placed under state surveillance in public places, whether overtly, or as some people might assume when protesting in public, covertly, and the idea that there is no reason to fear potential political victimisation from police surveillance. An appreciation of the extent to which police surveillance might have been a part of the long-term employment 'blacklisting' practices in the construction sector [72], or the way that undercover officers have been alleged (and have even admitted) to infiltrating protest groups contesting laudable causes such as police discrimination and victimisation itself[73], gives a different part of the jigsaw on police intelligence practices that Lord Sumption has overlooked.

There is also no sense of any recognition here of the argument that, for those who do feel retention of surveillance and intelligence records describing them is an intrusion by the state that warrants justification, the effect might be a 'chilling' of the desire to protest, and corollary reduction in the ability to utilise one's own freedom of expression. For Lord Sumption (at para. 31), criticisms or indeed fears and scepticism toward the purpose for retaining information on police databases:

"need to be considered in the light of some basic, and perhaps obvious, facts about the nature of intelligence-gathering. Most intelligence is necessarily acquired in the first instance indiscriminately. Its value can only be judged in hindsight, as subsequent analysis for particular purposes discloses a relevant pattern. The picture which is thus formed is in the nature of things a developing one, and there is not always a particular point of time at which one can say that any one piece in the jigsaw is irrelevant. The most that can be done is to assess whether the value of the material is proportionate to the gravity of the threat to the public."

There is instead a prominent consideration given to the issue of resources, costs and pragmatisms by Lord Sumption, who writes in *Catt* (at para. 32) that:

"The current weeding process in relation to nominal records involves an assessment of the threat posed by the subject of each such record. Mr Catt is not the subject of a nominal record, but merely appears as part of the cast in incidents with which the subjects of nominal records are associated. To fillet all the nominal records not simply in order to review the retention of information relating to the subject of the record but to examine the individual position of every other person mentioned in it would be a major administrative exercise. The alternative of not retaining information in a nominal record about any other members of the cast would significantly undermine the value of the record."

The current required scope of the 'administrative exercise' of reviewing then deleting or retaining police intelligence such as 'event histories' is set out in the guidance published by more than one relevant information

regulator; and it is this guidance to which the next Part of this piece now turns.

8. RECENT CHANGES TO GUIDANCE ON THE RETENTION AND DELETION OF POLICE RECORDS MADE FOLLOWING THE DECISION BY THE SUPREME COURT IN *CATT*

To a certain, more practical extent, the oversight and regulation of police intelligence databases is achieved through the self-regulation by the police of intelligence databases and the role of the relevant College of Policing guidance on 'Authorised Professional Practice' (or 'APP') [74], the relevant statutory Code of Practice in the form of the Management of Police Information guidelines [75], and the newly created guidance published by the National Police Chiefs' Council (the 'NPCC') on the deletion of records from police systems [76]. Importantly, sitting on top of this regulatory framework is the important constitutional notion that, in the UK at least, " [r]equests for the deletion of information which are refused are challengeable by way of judicial review." [77]

Recent guidance on the use, scope and retention of Police National Database and other local/specialised police records is to be found in the form of the latter document, produced by the NPCC (the inheritor of the regulatory role previously undertaken by ACPO, or the national Association of Chief Police Officers), which notes that:

"Locally held records, whether stored on other electronic document management systems or in manuscript, are managed by Chief Officers in accordance with Accredited Professional Practice (APP) [on] Information Management issued by the College of Policing. In this regard, it should be understood that this Guidance does not currently extend to the deletion of custody photographs." [78]

As for the aims of the NPCC, as the new quasi-regulator of police intelligence or criminality information management practices, their recent guidance observes, with a heavy nod towards the importance of compliance with both the law and central government policy, that:

"The Government wants to protect the civil liberties of innocent citizens, whilst giving police the powers they need to identify suspects and solve crime using DNA and fingerprints (hereafter referred to as biometric information). The Government also recognises that there is a requirement for the police to hold certain information about an individual's criminal antecedents for their policing purposes and to satisfy the requirements of criminal justice partners e.g. the courts. This information includes convictions, out of court disposals and other 'Event Histories'." [79]

With the *Catt* decision in the Supreme Court validating the status quo of criminality information or police intelligence designed as largely permanent, the NPCC have outlined the relative inflexibility and comprehensiveness they envisage for the single largest repository of data used by the police:

"PNC records are retained until a person is deemed to have reached 100 years of age. However, Chief Officers can exercise their discretion, in exceptional circumstances, to delete conviction records, specifically those relating to non-court disposals e.g. adult simple cautions and conditional cautions as well as any 'Event History' owned by them on the PNC but only where the grounds for so doing have been examined and agreed… A person may have an 'Event History' recorded on the PNC even though they have only come to the attention of the police, LEA or NPPA on one occasion and regardless of whether that one occasion resulted in the person being convicted of an offence." [80]

There are some criticisms we might make of the wording of the recent NPCC guidance, in an Appendix outlining factors affecting decisions to delete records from the PNC, however. This Appendix to the guidance asserts that:

"There is no set criterion for the deletion of records e.g. "beyond reasonable doubt" or "balance of probabilities"; it is for Chief Officers to exercise professional judgment based on the information available." [81]

But this assertion (which is about the standard of proof required to convince the chief officer concerned to order a deletion) is flawed. *Diktats* about a threshold for a standard of proof, which should rightly be the 'balance of probabilities' in a matter of determining civil rights, such as this, should also only be an assertion about the necessary certainty with which a chief officer must appreciate the component elements of the pertinent factual circumstances of an applicant seeking the deletion of the removal, and when weighing them in the balance. The decision as to whether to delete or retain data on the PNC following an application by an individual to have it removed must be a decision based on the key requirements of necessity, legitimacy and *proportionality*, and chiefly the latter, when appreciating those factual circumstances. This key paragraph in an appendix to the relevant guidance somewhat disastrously undermines the rights of potential applicants seeking the deletion of their PNC records, or 'Event Histories'.

Another element of the wording of the recent NPCC guidance is somewhat at odds with the rationale deployed by the majority of the Supreme Court in deeming the retention of police intelligence records about John Catt to be justifiable and therefore lawful. While in the *Catt* judgment Lord Sumption, and to a lesser extent other Supreme Court justices, actually acknowledged the risks posed by certain groups of (potential) offenders in society as a justification for retaining information about their associates more broadly, the NPCC guidance actually states that:

" Chief Officers will consider applications on an individual basis and will not set retention periods for groups of individuals, however defined. "[82]

And rightly so, since to do otherwise would arguably be an unlawful 'fettering of discretion' by the chief police officer who did engage in this kind of group profiling. But where does this leave our understanding of the supposed need to retain information about individuals on the fringes of organised crime, terrorism, drug distribution and football hooliganism, as per Lord Sumption in *Catt*, however? In many ways it could be said that *Catt* has done little but create a concern over the potential chilling effect of the judgment on the enjoyment of the right to protest in public.

9. CONCLUSION: LOOKING AHEAD

In reality, legalities of police retention of personal information, whether as 'criminality information', or 'police intelligence' data, are never going to be completely settled. Technological advances in the field of intelligence gathering, recording and data analysis alone would see to that, we suspect.

The resources issue, in terms of the higher costs that would come with the more nuanced 'weeding' of records, combines powerfully with arguments for the use of fully comprehensive intelligence databases to help the police protect the public, in the face of any privacy rights or civil liberties arguments to the contrary. And yet those latter arguments, in favour of stronger and continuous police accountability over the regulation of 'criminality information' and the retention of records identifying individuals on intelligence databases, must nonetheless continue to be made.

We would tentatively suggest a number of conclusions and recommendations arrived at through our discussion in this piece of both the law relating to police intelligence and evolving police regulatory guidance on the retention of that police intelligence:

There is a lack of definition around the notion of police intelligence itself, both in case law and in guidance and policy (as 'soft law'). It can mean information collected in the course of investigations, or it can mean the product of analysis (intelligence products) used to draw inferences and conclusions, and make decisions. The retention of unassessed intelligence could be viewed as less intrusive than interpreted or assessed intelligence (for instance, retaining the fact that Mr Catt attended a demonstration is less intrusive than recording him as an associate of violent demonstrators with the implicit label that this suggests). We conclude that criteria in case law and regulatory guidance for intelligence retention lack clarity and coherence. We believe that not enough attention has yet been paid to existing and potential electronic data analysis techniques. Further cases are inevitable, and future applicants may well use *Davis* to support an argument for independent review of retention decisions. Ultimately case law is not the appropriate vehicle to which police decision-makers should refer. The Government needs to address, through regulation or code, the extent to which information about all of us is 'on the radar' while ensuring that safeguards exist to prevent misuse of the microscope. There are worse starting points than those criteria for the governance of criminality information sharing, as identified by Lord Neuberger in *L* and recently endorsed by Mr Justice Behrens in *SD*, of reliability; gravity; relevance; currency; impact; and the overall proportionality of the sharing (and here the retention) of information.

Furthermore, there appears to be a lack of corporacy in the management of information across police forces, suggesting the need for primary legislation covering both the definitions, and the ongoing retention and use of categories of information in order to improve consistency of approach. It would be advisable for such statutory framework to go further than asking Chief Constables to *have regard* to the rules. Chief Constables may resist any suggestion of compulsion, but as the technological aspects of policing become ever more important, so does the importance of ensuring that information accessed is accurate and relevant. Such statutory framework would inevitably need to address the difficult arguments as to when information, and in particular intelligence, should be deleted, forcing an acceptance that forces must be prepared to delete in some circumstances, despite the risk to future investigations. Just as importantly, any new framework must facilitate the police's ability to make valuable links across records in different forces and at the same time, restrict an individual force's ability to make unilateral, blanket or automated decisions about deletion of certain records.

One uncertainty on a practical level that the *Catt* decision in the Supreme Court has created is with regard to the regulatory and oversight role that the Information Commissioner's Office [83] will have in relation to police intelligence databases in the future, after obiter dicta in *Catt* (at para. 45), where Lord Sumption observed that: "the parties [in *Catt*] have gone through three levels of judicial decision, at a cost out of all proportion to the questions at stake."

Indeed, the recent guidance from the NPCC on the process for potential deletion of police records states that

"A person affected by the processing of personal data can request an assessment from the Information Commissioner on whether the retention and processing of their personal data complies with DPA requirements… If the Information Commissioner is asked to make an assessment the Chief Officer should provide all the information that the Information Commissioner reasonably requires to make the assessment… If the Information Commissioner determines that the processing is likely to contravene the DPA then the Chief Officer must review the original decision to retain the relevant records having due regard to the Information Commissioner's assessment." [84]

We wonder though if the ICO is best equipped (or resourced) to deal with challenging and specialist necessity and proportionality human rights arguments. There is no single independent oversight body for police databases, since their operation is regulated by a combination, in practice, of the College of Policing, the NPCC, HMIC, the Home Office, and more than 40 police forces all across the UK - not to mention legal oversight from the courts and the ICO. There has been a proposal by the Independent Surveillance Review for a single National Intelligence and Surveillance Office [85]; and the oversight, governance and accountability functions of this body could be extended to cover the retention of police intelligence on databases as well as interception of communications/bulk communications data. In addition or in the alternative, there may well be room for an Information Management Commissioner, independent from the Inspectorate function, with a role to motivate and assist police forces with information management requirements. Such bodies are likely to uncover inconsistencies in approach due to the sheer number of police authorities, all independently making decisions about retention. This adds another dimension to the finely balanced debate over the desirability of a national police force in England and Wales. [86]

---

[1]

We are grateful to Ian Readhead, CEO of ACRO and Director of Information, for his comments on the policy issues discussed in this article.

[2] *R (Catt and T) v Commissioner of Police of the Metropolis* [2015] UKSC 9, at [1].

[3] See http://www.npcc.police.uk/NationalPolicing/NDEDIU/AboutNDEDIU.aspx [Last accessed 27 July 2015]

[4] *Catt* at para 20

[5] *In the matter of an application by JR38 for judicial review (Northern Ireland)* [2015] UKSC 42

[6] *JR38* at para 21

[7] See for example *Liberty v Secretary of State for Foreign and Commonwealth Affairs* [2015] UKIPTrib 13_77-H and *Davis v The Secretary of State for the Home Department* [2015] EWHC 2092 (Admin)

[8] David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf [Last accessed 27 July 2015]

[9] As Lord Brown observed in *R (Laporte) v Chief Constable of Gloucestershire* [2006] UKHL 55, unrestrained police powers may have a "potentially chilling effect on freedom of assembly and expression".

[10] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015, 21

[11] *Intelligence management* , Authorised Professional Practice, College of Policing, October 2013. Available at https://www.app.college.police.uk/app-content/intelligence-management/ [Last accessed 5 July 2015]

[12] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015, 19

[13] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015, 20

[14] *Intelligence-Led Policing: The New Intelligence Architecture* , Bureau of Justice Assistance, September 2005, at 3, available at https://www.ncjrs.gov/pdffiles1/bja/210681.pdf [Last accessed 27 July 2015]

[15] https://www.mi5.gov.uk/home/about-us/how-we-operate/gathering-intelligence.html

[16] *College of Policing (2015): Intelligence products [Internet]. https://www.app.college.police.uk/app-content/intelligence-management/intelligence-products/ [Last accessed 05 July 2015]*

[17] *Catt* at para 31

[18] *College of Policing (2014) : Research and analysis [Internet]. https://www.app.college.police.uk/app-content/intelligence-management/analysis/ [Last accessed 05 July 2015]*

[19] See https://www.app.college.police.uk/app-content/national-decision-model/the-national-decision-model/#information-gather-information-and-intelligence [Last accessed 25 July 2015]

[20] *Intelligence-Led Policing: The New Intelligence Architecture* , Bureau of Justice Assistance, September 2005, at 7, available at https://www.ncjrs.gov/pdffiles1/bja/210681.pdf

[21] Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI), Whitehall, 8 October 2013, available at https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-at-rusi-2013.html [Last accessed 27 July 2015]

[22] Helen Nissenbaum, *Privacy in Context*, Stanford University Press (2010), 41

[23] Helen Nissenbaum, *Privacy in Context*, Stanford University Press (2010), 42

[24] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015, 25

[25] Helen Nissenbaum, *Privacy in Context*, Stanford University Press (2010), 42

[26] Mireille Hildebrandt, *Smart Technologies and the End of Law: Novel Entanglements of Law and Technology*, Edward Elgar (2015), viii

[27] *A Democratic Licence to Operate* : Report of the Independent Surveillance Review, July 2015, para 2.14 available at https://www.rusi.org/downloads/assets/ISR-Report-press.pdf [Last accessed 27 July 2015]

[28] Jamie Grace, 'The surveillance of 'risky subjects': adiaphorisation through criminal records, and contested narratives of stigma', (2014) 2(2) *Birkbeck Law Review*, 279-292

[29] Jamie Grace, 'Privacy, stigma and public protection: A socio-legal analysis of criminality information practices in the UK', *International Journal of Law, Crime and Justice* 41 (2013) 303-321

[30] As Atina Krajewska has written in her article 'The right to personality in (post)-genomic medicine: a new way of thinking for the new frontier' (E.H.R.L.R. 2011, 1, 54-70), the right to informational self-determination, or 'Recht auf informationelle Selbstbestimmung' in German legal

theory and culture 'puts the individual in the position to, in principle, decide for him/herself which personal information is to be disclosed in his/her social environment.' (66).

[31] The Anderson report noted at p.130 that: "There are limits to what the public will (or should) take on trust."

[32] See Daniel J. Solove, *Nothing to Hide*, Yale University Press (2011), 33

[33] Anderson report at p.245

[34] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) [2014] 3 W.L.R. 1607 (ECJ (Grand Chamber))

[35] *Davis v The Secretary of State for the Home Department* [2015] EWHC 2092 (Admin). Since the date of writing, the Court of Appeal has ruled in the Government's appeal against the Davis judgment holding that the Divisional Court was wrong to conclude that Digital Rights Ireland laid down mandatory requirements in relation to access to retained communications data, and referring two questions to the CJEU: Secretary of State for the Home Department v David Davis MP and others [2015] EWCA Civ 1185

[36] See Ministry of Justice, *Government response to the House of Commons European Scrutiny Committee Report, 43rd \ Report, 2013-14, HC979, The application of the EU Charter of Fundamental Rights in the UK: A State of Confusion* , from https://www.gov.uk/government/publications/government-response-to-the-application-of-the-eu-charter-of-fundamental-rights-in-the-uk-a-state-of-confusion (Last accessed 25 July 2015).

[37] Nigel Morris, ' Question that voters will be asked in EU Referendum Bill revealed', http://www.independent.co.uk/news/uk/politics/eu-referendum-vote-on-uk-membership-to-be-rushed-into-law-extraquick-time-10279730.html (Accessed at 25/07/15)

[38] Steve Foster, 'Repealing the Human Rights Act - no not delay, just don't do it', Cov. L.J. 2015, 20(1), 9-16

[39] See for example *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2015] UKIPTrib 13_77-H_2 that swiftly followed the report by David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015.

[40] See Jamie Grace, 'The surveillance of 'risky subjects': adiaphorisation through criminal records, and contested narratives of stigma', (2014) 2(2) *Birkbeck Law Review*, 279-292

[41] Jamie Grace, 'The surveillance of 'risky subjects': adiaphorisation through criminal records, and contested narratives of stigma', (2014) Vol. 2 Issue 2 *Birkbeck Law Review*, 279-292, 284.

[42] J. Grace, 'Old convictions never die, they just fade away: The permanency of convictions and cautions for criminal offences in the UK', J. Crim. L. 2014, 78(2), 122-136, 122.

[43] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015, p.36

[44] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015, p.37,43

[45] *A Democratic Licence to Operate* : Report of the Independent Surveillance Review, July 2015, para 3.62 available at https://www.rusi.org/downloads/assets/ISR-Report-press.pdf [Last accessed 27 July 2015]

[46] See https://www.app.college.police.uk/app-content/intelligence-management/analysis/ (Last accessed 25 July 2015)

[47] See, most recently, *R (SD) v Chief Constable of North Yorkshire* [2015] EWHC 2085 (Admin)

[48] Graeme Laurie, and Nayha Sethi, 'Towards principles-based approaches to governance of health-related research using personal data', *European Journal of Risk Regulation: EJRR* 4.1 (2013): 43.

[49] See commentary throughout *Building the picture*, Her Majesty's Inspectorate of Constabulary, July 2015.

[50] Marion Oswald, 'Joining the dots - intelligence and proportionality', P. & D.P. 2013, 13(5), 6-8, 8.

[51] For context, see Ed Cape, ' The Protection of Freedoms Act 2012: the retention and use of biometric data provisions', Crim. L.R. 2013, 1, 23-37.

[52] This seems to us rather ironic considering how difficult it would be, or frankly near-impossible, for any private individuals to obtain any personal data from DNA.

[53] The second claimant in the *Catt* litigation before the Supreme Court was T, whose claim was also ultimately unsuccessful, and who was challenging the retention for up to 7 years of a letter recording her warning by the Metropolitan Police over an alleged incident of homophobic harassment. A record of the allegation itself was originally to be retained under a policy determined by the Met for up to 12 years. The Met actually deleted the information about T that was the subject of her claim during the course of proceedings.

[54] Again, see *Building the picture*, Her Majesty's Inspectorate of Constabulary, July 2015.

[55] In *R (RMC and FJ) v Commissioner of the Police of the Metropolis* [2012] EWHC 1681 (Admin), the High Court determined that the police retaining of photographs of the two claimants in police

custody following their arrest was disproportionate after they had not been charged in relation to the initially alleged offences.

[56] House of Commons Science and Technology Committee, *Current and future uses of biometric data and technologies*, Sixth Report of Session 2014-15, House of Commons: London, 25 February 2015, p.3

[57] See http://www.heraldscotland.com/news/13215304.Controversial_face_recognition_software_is_being_used_by_Police_Scotland__the_force (Last accessed 25 July 2015)

[58] While we observed in a previous note that in *R (RMC and FJ) v Commissioner of the Police of the Metropolis* [2012] EWHC 1681 (Admin), the High Court determined that the police retaining of photographs of the two claimants in police custody following their arrest was disproportionate after they had not been charged in relation to the initially alleged offences, an argument that the records of arrest of one of the two claimants, FJ, a child at the time, should be deleted from the Police National Computer (PNC) database, was rejected. This difference in treatment between the two media of photographs and textual records was justified by the High Court on the grounds that the PNC should, in effect, provide an accurate a record of the claimant's procedural interactions with the police.

[59] In *R (Catt) v Commissioner of the Police of the Metropolis* [2012] EWHC 1471 (Admin) at first instance, Gross LJ determined that Article 8 ECHR was not engaged since the surveillance used to record information about John Catt was deployed at a public event, and was visible and overt surveillance. Gross LJ also determined that if Article 8 ECHR had been engaged, the retention of the information for police intelligence purposes was justified on the basis that the group with which Catt was affiliated included a number of individuals who had themselves been violent at public protests.

[60] Marion Oswald, 'Joining the dots - intelligence and proportionality', P. & D.P. 2013, 13(5), 6-8, 8.

[61] College of Policing, 'How to complete a 5x5x5 form', http://library.college.police.uk/docs/APPref/how-to-complete-5x5x5-form.pdf , [Last accessed 5 July 2015]

[62] See Jamie Grace, 'Old convictions never die, they just fade away: The permanency of convictions and cautions for criminal offences in the UK', J. Crim. L. 2014, 78(2), 121-135.

[63] *R (Catt) v ACPO & Metropolitan Police* [2015] UKSC 9

[64] Marion Oswald, 'Joining the dots - intelligence and proportionality', P. & D.P. 2013, 13(5), 6-8, 7.

[65] *R (on the application of Catt and T)* v *ACPO and Metropolitan Police* [2013] EWCA Civ 192 at para. 7.

[66] *Building the picture* , Her Majesty's Inspectorate of Constabulary, July 2015.

[67] Registrar of the European Court of Human Rights (press release), 'French crime database system in breach of Convention for storing information on individuals against whom proceedings have been dropped', ECHR 263 (2014), 18.09.2014

[68] Case Comment, 'Police: non-conviction information retained on a national database - impossibility of review of decision to refuse to delete information', E.H.R.L.R. 2015, 1, 94-96, p.96

[69] *Davis v The Secretary of State for the Home Department*. Since the date of writing, the Court of Appeal has ruled in the Government's appeal against the Davis judgment holding that the Divisional Court was wrong to conclude that Digital Rights Ireland laid down mandatory requirements in relation to access to retained communications data, and referring two questions to the CJEU: Secretary of State for the Home Department v David Davis MP and others [2015] EWCA Civ 1185 [2015] EWHC 2092 (Admin).

[70] See David Hart QC, 'An ABC on proportionality - with *Bank Mellat* as our primer', from http://ukhumanrightsblog.com/2013/06/22/an-abc-on-proportionality-with-bank-mellat-as-our-primer/ (Last accessed 12 June 2015)

[71] Lord Mance agrees with the reasoning of Lord Sumption and Lady Hale in finding that the retention of data about John Catt was lawful; and with Lady Hale and Lord Toulson that retaining data about Ms T was lawful.

[72] See Dave Smith and Phil Chamberlain, *Blacklisted: The Secret War Between Big Business and Union Activists*, New Internationalist, March 2015

[73] See http://www.theguardian.com/uk-news/2015/jul/16/theresa-may-public-inquiry-undercover-police and http://www.theguardian.com/uk-news/2015/jul/15/doreen-lawrence-name-undercover-police-spied-family (Last accessed 25 July 2015)

[74] See https://www.app.college.police.uk/app-content/information-management/ (Last accessed at 25 July 2015)

[75] See https://www.app.college.police.uk/app-content/information-management/management-of-police-information/ (Last accessed 25 July 2015)

[76] See National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430095/Record_Deletion_Process.pdf (Last accessed 25 July 2015)

[77] Case Comment, 'Police: non-conviction information retained on a national database - impossibility of review of decision to refuse to delete information', E.H.R.L.R. 2015, 1, 94-96, p.96

[78] National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, p.1

[79] National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, p.3

[80] National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, p.4

[81] National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, p.A-1

[82] National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, p.A-1

[83] https://ico.org.uk/

[84] National Police Chiefs' Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)', NPCC, May 2015, p.12

[85] Royal United Services Institute, A Democratic License to Operate: Report of the Independent Surveillance Review, from https://www.rusi.org/downloads/assets/ISR-Report-press.pdf (Last accessed 25 July 2015); Recommendation 17

[86] Independent Surveillance Review Recommendation 5 suggests that "A national approach to policing in the digital era is necessary and long overdue. The police require a unified national digital policing strategy and the resources to deliver the capability to ensure digital investigations and intelligence capability", p.xv.