Data Protection in 2016: The new General Data Protection Regulation; the new Police Directive; damage, interpretation and disapplication in *Vidal-Hall*; and police retention/disclosure cases in the UK

Stephen Cragg QC

Monckton Chambers

20 June 2016

General Data Protection Regulation 2016

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (in force 24.5.16, applies from 25.5.18)

Art 8 EU Charter of Fundamental Rights

"1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council…shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

General Data Protection Regulations - objectives

1. Update EU data protection rules in line with technological developments
2. Enhance data protection rights for individuals

3. Modernise, simplify and harmonise regulation throughout the EU
4. The need for tougher penalties and better powers of enforcement
5. Extend regulation of data processing outside the EU

1. There is a need for modernisation and harmonisation. The current Directive (95/46/EC) - dates from 1995 (and was based on 1990 Commission proposal). There have been rapid technological developments and the scale of data sharing and collection has increased dramatically. Intelligent technology allows private and state use of personal data on an unprecedented scale. There is a wide variation in national implementation of Directive 95/46/EC, and a need to do away with legal uncertainty and current costly fragmentation.

2. Some of the main articles in the Regulation are as follows: with reference to the Information Commissioner's Office guidance issued in March 2016: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf :-

Article 25: Data protection "by design" & "by default"

3. Proper systems in place to ensure that the right kind of data is collected and processed (or not), taking into account "the state of the art", cost, inherent risks and scope, context and purpose of processing.

Article 17: The right to erasure ("Right to be forgotten")

4. The right to have data erased when its retention and processing is no longer lawful or legitimate: the right described in the *Google Spain* v *Agencia Española de Protección de Datos* Case C-131/12

Article 8: Collecting information about children: need for parents' consent.

5. The first time this has been included. What the ICO says:

> For the first time, the GDPR will bring in special protection for children's
> personal data, particularly in the context of commercial internet services such as social networking. In short, if your organisation collects information about children – in the UK this will probably be defined as anyone under 13 – then you will need a parent or guardian's consent in order to process their personal data lawfully. This could have significant implications if your organisation aims services at children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

Article 20 –The right to data portability

6. The right to be provided with the data held in a format which allows it to be transmitted directly to another controller if technically feasible. What the ICO says:-

> The right to data portability is new. This is an enhanced form of subject access where you have to provide the data electronically and in a commonly used format. Many organisations will already provide the data in this way, but if you use paper print-outs or an unusual electronic format, now is a good time to revise your procedures and make any necessary changes.

Articles 77-83 – Remedies and liabilities

7. As well as the right to make a complaint to a supervisory authority, and a judicial remedy thereafter, there is also a right in Article 80 to mandate not-for-profit organisation to bring a case on your behalf. What the ICO says:-

> The main rights for individuals under the GDPR will be:
> □ subject access,
> □ to have inaccuracies corrected,
> □ to have information erased,
> □ to prevent direct marketing,
> □ to prevent automated decision-making and profiling, and
> □ data portability.
> On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements.

Articles 33-34 – Duty to notify a breach to a supervisory body

8. Within 72 hours of the breach. What the ICO says:-

> …the GDPR will bring in a breach notification duty across the board. This will be new to many organisations. Not all breaches will have to be notified to the ICO – only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach.
>
> You should start now to make sure you have the right procedures in place
> to detect, report and investigate a personal data breach. This could involve assessing the types of data you hold and documenting which ones would fall within the notification requirement if there was a breach. In some cases you will have to notify the individuals whose data has been subject to the breach directly, for example where the breach might leave them open to financial loss. Larger organisations will need to develop policies and procedures for managing data breaches – whether at a central or local level. Note that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

9. Enforcement is further enhanced by increased responsibility and accountability and the need for data protection risk assessments (see the ICO's guidance https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf and the need for public authorities to employ data protection officers.

Police and Criminal Justice Data Protection Directive

10. The data protection reform package includes the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities ("the Police Directive"): Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

11. The Police Directive replaces the current data protection rules that are based on the Framework Decision 2008/977/JHA for the police and criminal justice sector. The Police Directive seeks to regulate the use of personal data for law enforcement purposes, specifically "for the purposes of prevention,

investigation, detection or prosecution of criminal offences, the execution of criminal penalties or the safeguarding against and the prevention of threats to public security."

12. Member States have two years (to 2018) to apply the Data Protection Regulation and to transpose and implement the "Police Directive".

13. Whilst trumpeting the rights to data protection for individuals (enshrined in Article 8 of the Human Rights Charter), the new Police Directive is also heralded for allowing for smoother exchange of information between Member States' police and judicial authorities. Criminal law enforcement authorities will no longer have to apply different sets of data protection rules according to the origin of the personal data. EU countries may set higher standards than those enshrined in the directive if they so wish.

14. As the EU FAQ section says:-

> This will save time and money and increase the efficiency in the fight against crime. Having more harmonised laws in all EU Member States will make it easier for our police forces to work together… improving cooperation in the fight against terrorism and other serious crime in Europe It establishes a comprehensive framework to ensure a high level of data protection whilst taking into account the specific nature of the police and criminal justice field.

15. Critics of the new regime argue that, from the point of view of individuals, there are almost no improvements on the current legal situation, and object to the fact that the Directive fails to differentiate between suspects, witnesses, guilty parties and victims as regards the protection of their fundamental rights: presumably it is thought that witnesses and victims should have greater protection. It is argued that the opportunity for greater harmonisation to strengthen citizens' rights has not been taken, and that greater co-operation and information exchange between police authorities should not be introduced without greater cross-border data protection standards for individuals.

16. Although it is said that individuals' personal data will be better protected, the principles applied are already familiar to anyone working in this area. Thus, all personal data should be processed lawfully, fairly, and only for a specific purpose. All law enforcement processing in the Union must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Supervision is to be ensured by independent national data protection authorities and effective judicial remedies must be provide.

17. Further concerns were expressed by the European Data Protection Superviser who commented in October 2015 that:-

In substance, the EU legislator should ensure that:

1. None of the provisions of the Directive decreases the level of protection that is currently offered by EU law -particularly the 2008 Council Framework Decision- and by the instruments of the Council of Europe.
2. The essential components of data protection, laid down in Article 8 of the Charter of the Fundamental Rights of the Union, are respected and that exceptions fulfil the strict test of proportionality, as specified in *Digital Rights Ireland*. In this Opinion, we point particularly on the principle of purpose limitation, on the right to access of individuals to their personal data and on the control by independent data protection authorities.
3. The essential components of data protection are included in the Directive and not left to the discretion of the Member States. [1]

18. The Directive also provides rules for the transfer of personal data by criminal law enforcement authorities outside the EU, to ensure that these transfers take place with an adequate level of data protection. The directive provides rules on personal data exchanges at national, European and international level.

19. The directive also complements recent agreements on a new Europol regulation and the directive establishing a system collecting flight passenger data in the EU (EU PNR) by setting high, uniform standards on data transfers for law enforcement purposes. The Directive will cover the use of personal data for law enforcement purposes not just by the police. Other public organisations tasked

[1] Opinion 6/2015

with tackling crime, including local authorities with statutory prosecutorial functions will also be covered.

20. The position in the UK is complicated because the UK government has an opt-out in respect of the application of European data protection legislation in relation to domestic law enforcement. Due to the UK and Ireland's special status regarding Justice and Home Affairs legislation, the directive's provisions will only apply in these countries to a limited extent, that is only in the areas where the UK and Ireland have "opted in" to other laws on police and judicial cooperation. Outside of these areas, UK and Ireland will not be bound by the directive.

21. In practice, the UK will be bound by the Directive, when adopted, to permit the sharing of personal data for law enforcement purposes with other member states. However, the opt out applies to the Directive as it affects processing of personal data for law enforcement purposes in the UK itself.

22. The government's keenness to retain control of sovereignty over criminal justice issues means that a revocation of the opt out is unlikely. Other options to fill the gap have been suggested such as extending the GDPR to cover domestic law enforcement issues, or the consideration of new data protection legislation to cover criminal justice issues. There is the potential that public bodies using data for criminal justice/law enforcement purposes could be governed by three different regimes, depending on whether the data is covered by the GDPR, domestic law enforcement provisions, or the Directive (so far as sharing information with other members and beyond is concerned).

Vidal- Hall v Google

23. In *Vidal-Hall v Google* [2015] 3 WLR 409, CA the lead claimant, along with two others, was pursuing claims that Google, through its use of internet 'cookies', misused her private information, breached her confidence and infringed the Data Protection Act 1998 (DPA 1998).

24. The claimants complained that Google collected private information about their internet usage (the Browser-Generated Information - "BGI") via the Apple Safari browser, and without their knowledge and consent, by means of cookies. The cookies were small programmes which allowed Google to identify and categorise information generated by the claimants' use of their Apple Safari internet browsers, and subsequently target advertising based on the claimants' browser use.

25. This revealed private information about the claimants, which was or might have been seen by third parties. This was also contrary to Google's stated position that such activity could not be conducted for Safari users unless they had expressly allowed it to happen. The claimants' claims concerned the internet usage period between summer 2011 and spring 2012. None of the Claimants alleged any pecuniary loss or other material damage (not even nominal damages). Their claims were for damages or compensation for distress.

26. The case raised issues as to the meaning of "damage" in section 13 of the DPA 1998, in particular, whether there can be a claim for compensation without pecuniary loss. Section 13(2) DPA 1998 makes it clear that compensation can only be awarded for distress caused by a contravention of the DPA 1998 where an individual has also suffered other damage or where the contravention relates to the processing of personal data for the "special purposes" (as listed under the DPA 1998).

27. The DPA 1998 was intended to implement Directive 95/46/EC 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data'.

28. A number of articles in the Directive emphasise the importance of protecting "*the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" (see Article 1).*

29. Article 23 states that:-

> Member states *shall provide that any person who has suffered damage* as a result of an unlawful processing operation or of any act incompatible

> with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

30. In *Vidal-Hall* the claimants accepted that they had been caused no other damage other than distress by the contravention of the DPA (not even to justify the award of nominal damages). It was also accepted that a literal interpretation of s13 DPA must exclude them from compensation under the DPA, as they had suffered no pecuniary loss, and they did not come within exceptions in s13(2) DPA 1998.

31. The issues were considered thereafter by the Court of Appeal as follows:-

Does "damage" in article 23 include non-pecuniary loss?

32. As the DPA 1998 is designed to transpose the Directive, the question arose as to whether 'damage' in article 23 of the Directive included non-pecuniary loss. Google submitted that it did not. In support they cited Rosemary Jay "Data Protection Law and Practice"[2]:-

> …There is no reference to moral damages in the Directive. Article 23 provides that member states shall provide that any person who suffers damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. There is no presumption in EU law that the term 'damages' includes moral damages. Nothing in the recital to the Directive refers to moral damage. ….it can be strongly argued that there is no such obligation as long as the domestic legal system provides an effective set of remedies. Moreover the fact that awards can be made for distress (the moral damage equivalent) where the breach involves the literary, journalistic or artistic purposes would argue that any reputational damage is likely to be covered."

[2] 4th edition, 2012, para 14-34.

33. Also cited was the Irish case of *Collins v FBD Insurance plc*[3], where Feeney J commented that s13(2) of the DPA 1998, when providing for damages for distress in some circumstances, "goes beyond the requirements in the Directive.

34. However, the Court reached the opposite conclusion, taking the following steps in its reasoning:-

(a) The Court noted the principle of EU law that legal terms have an autonomous meaning which will not necessarily accord with their interpretation in domestic law (paragraph 72).

(b) The Court referred to the case *Leitner v TUI Deutschland GmbhH & Co K*[4] when considering the meaning of "damage", where Directive 90/314/EEC on package travel was engaged. The Advocate General in that case noted that where "damage" was used in a Directive without any restrictive connotation, then "the concept should be interpreted widely". The ECJ itself found that as "compensation for non-material damage arising from the loss of enjoyment of a holiday is of particular importance to consumers", then that was important to the way "damage" in that Directive should be interpreted.

(c) The Court of Appeal thus took the same approach to the construction of "damage" in article 23 of the Directive 95/46/EC (paragraph 76). Importantly, the court concluded that:-

> Since what the Directive purports to protect is privacy rather than economic rights, it would be strange if it could not compensate individuals whose data privacy had been invaded so as to cause emotional distress (but not pecuniary damage). It is the distressing invasion of privacy which must be taken to be the primary form of damage (commonly referred to in the European context as 'moral damage') and the data subject should have an effective remedy (paragraph 77).

[3] [2013] IEHC 137
[4] (case C-168/00) [2002] All ER (EC) 561

(d) The Court also decided that it was irrational to treat EU data protection law as permitting a more restrictive approach to the recovery of damages than is available under article 8 of the ECHR: the object of the Directive[5] was to ensure that data-processing systems protect and respect the fundamental rights and freedoms of individuals. The enforcement of privacy rights under article 8 of the ECHR has always permitted recovery of non-pecuniary loss.[6]

(e) The Court also considered article 8 of the Charter of Fundamental Rights[7], and commented that:-

> It would be strange if that fundamental right could be breached with relative impunity by a data controller, save in those rare cases where the data subject had suffered pecuniary loss as a result of the breach. It is most unlikely that the member states intended such a result (paragraph 78)

(f) On that basis the court concluded that article 23 of the Directive does not distinguish between pecuniary and non-pecuniary damage. To make the distinction "would substantially undermine the objective of the Directive which is to protect the right to privacy of individuals with respect to the processing of their personal data". The Court even rejected a suggestion by Ms Vidal-Hall's counsel that non-pecuniary damage should only extend to cases where there was also a breach of Article 8 of the ECHR.

The construction of section 13(2) of the 1998 Act

35. So what to do about the literal construction of section 13(2) of the DPA which, on the Court's finding on the meaning of "damage", failed to transpose Article 23?

36. The Court considered whether it was possible to "interpret section 13(2) in a way which was compatible with article 23 so as to permit the award of compensation for distress even in circumstances which do not satisfy the

[5] Recitals (2), (7), (10) and (11) and Article 1 were especially referred to: all emphasise the right to privacy.
[6] Although not always awarded: see for example the applicants in *S v UK* (2009) 48 EHRR 50 (the DNA case) were not awarded anything for the indefinite retention of their DNA samples and fingerprints.
[7] "Everyone has the right to the protection of personal data concerning him or her."

conditions set out in section 13(2) (a) or (b)". The claimants and defendant agreed it was not possible (although the Information Commissioner argued, unenthusiastically by the sounds of things, that it could).

37. The Court of Appeal took the following route:-

(a) The *Marleasing* principle is that the courts of Member States should interpret national law enacted for the purpose of transposing an EU directive into its law, so far as possible, in light of the wording and the purpose of the directive in order to achieve the result sought by the directive, the critical words being 'so far as possible'.

(b) If it is not possible to do this, even where it is clear that the legislation intended to implement the directive, the appropriate remedy for an aggrieved person is to claim *Francovich* damages against the state.

(c) The court recognised a close parallel between the *Marleasing* principle and section 3 of the HRA,[8] and "by analogy with the approach to section 3 of the HRA, the court cannot invoke the *Marleasing* principle to adopt a meaning which is 'inconsistent with a fundamental feature of the legislation'" (paragraph 83).

(d) The jurisprudence of the Court of Justice recognises that when transposing a directive a Member State may choose not to implement it faithfully. The court considered it clear that Parliament had deliberately chosen to limit the right to compensation but was unable to ascertain why.

(e) A number of interpretive "techniques" could be used to try to eliminate an incompatibility. These include reading words in, reading down, and even disapplying or striking down part of a measure. Whether any of these approaches can be used depended on " whether the change brought about by the interpretation alters a fundamental feature of the legislation or is inconsistent with its essential principles or goes against its grain, to use Lord Rodger's memorable phrase". (paragraph 90).

[8] And cited R (IDT Card Services Ireland Ltd) v Customs and Excise Comrs [2006] STC 1252, para 92.

(f) No one had suggested that the exclusion of distress in most circumstances was an oversight from section 13 DPA 1998, even though it had not been possible to determine why Parliament had excluded it. The Court decided that section 13 is a central feature of the DPA 1998 and section 13(2) is an important element of the compensation provisions that Parliament enacted. In view of the importance to the DPA scheme as a whole of the provisions for compensation, the limits set by Parliament in that regard are a fundamental feature of the legislation. (paragraph 93).

(g) On that basis, whatever technique was used, the court decided that it could not, therefore, interpret section 13(2) compatibly with article 23.

Article 47 of the Charter of Fundamental Rights of the European Union

38. Article 47 of the Charter provides:-

> "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article'.

39. Article 7 of the Charter provides that 'everyone has the right to respect of his or her private and family life, home and communications', and as stated above article 8(1) of the Charter provides that 'everyone has the right to the protection of personal data concerning him or her'. The claimants and the Information Commissioner argued that section 13(2) DPA 1998 should be disapplied on the grounds that it conflicts with the rights guaranteed by articles 7 and 8 of the Charter and the court accepted that submission.

40. The Court of Appeal explained its conclusion as follows:-

(a) The approach in *Benkharbouche*[9] was applicable. Thus:-

[9] *Benkharbouche v Embassy of the Republic of Sudan* [2016] QB 347

i. where there is a breach of a right afforded under EU law, article 47 of the Charter is engaged;

ii. the right to an effective remedy for breach of EU law rights provided for by article 47 embodies a general principle of EU law;

iii. in most cases, that general principle has horizontal effect;

iv. in so far as a provision of national law conflicts with the requirement for an effective remedy in article 47, the domestic courts can and must disapply the conflicting provision; and

v. the only exception to iv. is that the court may be required to apply a conflicting domestic provision where the court would otherwise have to redesign the fabric of the legislative scheme.

(b) The Court rejected Google's arguments against this approach, stating:-

i. Article 8 is based on the Directive and therefore the claimants were not relying upon Charter rights to expand their EU rights (which the Court accepted would be impermissible).

ii. Provisions in the DPA 1998 for the Information Commissioner to serve an enforcement notice and/or impose a monetary penalty, cannot make good the failure of s13(2) to provide, in most cases, for compensation for distress.

iii. The reliance on *R (Chester) v Secretary of State for Justice*,[10] to prevent the court disapplying a carefully calibrated Parliamentary choice, was misplaced.

(c) In relation to the last point, the defendants relied upon the rejection by Lord Mance in the Supreme Court in *Chester* that it should disapply the whole of the

[10] [2014] AC 271.

legislative prohibition on prisoner voting, so as to make all prisoners eligible to vote in order, (as that was not what was required to comply with EU law). The Supreme Court said also that it could not interpret the relevant legislation compatibly because that would entail devising a scheme allowing some prisoners to vote and that was quintessentially a matter for Parliament. However, the Court of Appeal noted that:-

> It is implicit in Lord Mance JSC's reasoning that, if EU law did not permit any prohibition on prisoner voting, the proper course would have been to disapply the relevant legislation (paragraph 103).

(d) The Court of Appeal decided that, as in *Benkharbouche*, the scope of the disapplication was clear:-

> What is required in order to make section 13(2) compatible with EU law is the disapplication of section 13(2), no more and no less. The consequence of this would be that compensation would be recoverable under section 13(1) for *any* damage suffered as a result of a contravention by a data controller of any of the requirements of the DPA. No legislative choices have to be made by the court.

41. Thus the Court of Appeal completed a fancy piece of footwork. S13(2) was a fundamental aspect of the DPA, such that it was not possible use interpretive techniques to make it comply with Article 23. But that did not prevent the Court disapplying s13(2) completely to comply with Article 47, because the disapplication was of a self-contained aspect of the DPA 1998.

Appeal to the Supreme Court

42. Google has been granted permission to appeal to the Supreme Court on the following grounds:

> Whether the Court of Appeal was right to hold that section 13(2) of the Data Protection Act 1998 was incompatible with Article 23 of the Directive.
>
> Whether the Court of Appeal was right to disapply section 13(2) of the Data Protection Act 1998 on the grounds that it conflicts with the rights guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights.

43. The case raises an interesting issue in relation to cases which engage fundamental rights under both the ECHR and the Charter. The practical effect of the Court's conclusion is to grant a claimant potentially stronger remedies under EU law for human rights breaches: disapplication of primary legislation, rather than a mere declaration of incompatibility under s.4 of the Human Rights Act 1998.

The police and data protection/use in the UK – 2008 -2016

44. There has been a series of cases over the last eight or nine years focussing on police powers in the UK to retain, disclose or otherwise use personal information and citing both ECHR and EU law.

S v UK (2008) 48 EHRR 1169

45. Indefinite retention of DNA samples and fingerprints was a breach of Article 8, said the Grand Chamber. Given the nature of personal information contained in cellular samples, their retention per se had to be regarded as interfering with the right to respect for the private lives of the individuals concerned.

46. The Court said that retention had a clear basis in domestic law and pursued a legitimate aim. However, it failed to achieve a fair balance between the respective public and private interests.

> 119 In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; …The retention is not time limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed ; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

47. A particular concern was the risk of stigmatisation, in that innocent individuals were treated in the same way as convicted persons, which raised an issue as to their perception of the presumption of innocence.

R (L) v Metropolitan Police Commissioner [2010] 1 AC 410

48. L had been employed as an assistant at a school, supervising children in the lunchtime break. An ECRC was disclosed that her son had been placed on the child protection register under the category of neglect, she being alleged to have failed to exercise the requisite degree of care and supervision. As a result, L lost her job. She sought the quashing of the police decision to disclose the information together with a declaration that the relevant statutory provisions were incompatible with her article 8 rights.

49. The Court held that in forming the opinion on relevance, the police had to consider, whether the information "ought" to be included in the ECRC. The police had therefore to consider in every case whether there was likely to be an interference with the applicant's private life, and if so whether that interference could be justified. The issue was essentially one of proportionality. On the one hand there was a pressing social need that children and vulnerable adults should be protected against the risk of harm; on the other there was the applicant's right to respect for her private life. The correct approach was that neither consideration had precedence over the other. Lord Hope at para 27:-

> …..information about an applicant's convictions which is collected and stored in central records can fall within the scope of private life within the meaning of article 8(1) , with the result that it will interfere with the applicant's private life when it is released. It is, in one sense, public information because the convictions took place in public. But the systematic storing of this information in central records means that it is available for disclosure under Part V of the 1997 Act long after the event when everyone other than the person concerned is likely to have forgotten about it. As it recedes into the past, it becomes a part of the person's private life which must be respected. Moreover, much of the other information that may find its way into an ECRC relates to things that happen behind closed doors. …..It may even disclose something that

could not be described as criminal behaviour at all. The information that was disclosed on the appellant's ECRC was of that kind.

R (GC) v Commissioner of the Police for the Metropolis [2011] 1 WLR 1230

50. Two appellants who had been arrested and not convicted claimed that their DNA samples and fingerprints had been retained by the police indefinitely under a policy promulgated by ACPO which the House of Lords in 2004 held was lawful : *R (S) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196, but which the Grand Chamber of the ECtHR decided in December 2008 was a blanket and indiscriminate policy which amounted to a breach of Article 8 ECHR: *S and Marper v United Kingdom* (2008) 48 EHRR 1169.

51. A seven member panel of the Supreme Court decided that it should follow the Grand Chamber's approach and that it should depart from the House of Lords decision. Thus, the indefinite retention of the claimants' data was an unjustified interference with their rights under article 8 of the Convention.

R (on the application of C) v Metropolitan Police Commissioner [2012] EWHC 1681 (Admin) [2012] 1 WLR 3007

52. The Divisional Court decided that it was disproportionate for the Metropolitan Police to retain photographs taken on arrest in the police station for long periods of time (at least six years before a review) in cases where the individual was subsequently not charged and/or not convicted of any offence.

53. The Force said that it was applying a Code of Practice and guidance drawn up by Home Office for the management of information by the police. But the Court declared that approach was incompatible with the Claimants' rights to respect for private life pursuant to Article 8 of the European Convention of Human Rights. It did not order that the photographs be destroyed on the basis that the Force said it was revising the policy, but the Court made it clear that a new policy would be expected within months rather than years. (New policy still awaited!)

54. The Biometrics Commissioner (who oversees the use of DNA samples and fingerprints but not photographs) has recently expressed wide-ranging concerns about the retention of photographs on the national database, the total lack of regulation that applies, and the decision of the police to introduce upload photographs to the database without further public debate or national consultation. www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014

R (T) v Chief Constable of Greater Manchester and R (B) v Secretary of State for the Home Department [2014] UKSC 35. [2014] 3 WLR 96.

55. The Supreme Court upheld the Court of Appeal's conclusions that the obligation to disclose all cautions for the purposes of criminal records checks, as set out in Part V of the Police Act 1997 was incompatible with Article 8 rights to respect for private life, as were the disclosure provisions in the Rehabilitation of Offenders Order 1975.

56. The Supreme Court had little trouble finding that the relevant provisions interfered with T's and B's Article 8 ECHR rights and had "*significantly jeopardised entry into their chosen field of endeavour*".

57. In relation to the disclosure of data relating to T's and B's cautions under the 1997 Act, the majority of the UKSC took the view that the interference was not "*in accordance with the law*" within the meaning of Article 8(2) ECHR, and was therefore unlawful. The reasoning in this regard appears in the judgment of Lord Reed. Relying on the case of *MM v UK* (App. No. 24029/07), which concerned the disclosure of an individual's conviction for child abduction pursuant to a version of the 1997 Act which was materially identical to that considered in the case of T and B, he held: ."..*That judgment establishes, in my opinion persuasively, that the legislation fails to meet the requirements for disclosure to constitute an interference "in accordance with the law".*

58. There was unanimity amongst the judges that the interference with T's and B's Article 8 ECHR rights arising from both the 1997 Act and the 1975 Order was not necessary in a democratic society, and therefore unjustified. Lord Wilson considered that the legislative provisions served the "*supremely important*" objective of protecting various members of society, particularly vulnerable groups. Nonetheless, it was noted that T's and B's criticism of the regime was "*obvious*". Of particular force was the point that the regime operated "*indiscriminately*". The Court concluded that the regime set up by the 1997 Act and the 1975 Order failed the requirement of necessity, going further than was necessary to accomplish the statutory objective, and failing to strike a fair balance between T's and B's rights and the interests of the community.

R (Catt), R (T) v Commissioner of Police of the Metropolis [2015] A.C. 1065

59. These were appeals to the Supreme Court by Mr Catt, 91, who complained about retention of information by the police about his presence at demonstrations where they had been violence (although not from him); and by T who objected to a policy of retention of an harassment warning by police for seven or twelve years. The Court of Appeal had decided that the actions of the police in both cases were disproportionate breaches of the right to respect for private life by the police

60. The Supreme Court decided Article 8 was engaged in both cases. The majority decided that given the context in Mr Catt's case, the interference with his Article 8 rights was minimal and that the retention was justified for the purposes of intelligence-gathering in relation to public order offences. Long periods of retention of harassment notices could not be justified in T's case, but as in fact the notice had been destroyed after 2 ½ years in her case, there was no breach of Article 8: retention for that period was justified in case there were repeated actions of harassment in that period.

Gaughran v Chief Constable of Northern Ireland [2015] UKSC 29

61. This case from Northern Ireland considered the proportionality of indefinite retention of DNA samples, profiles and other information including photographs and fingerprints, where a person has been convicted of a recordable offence. The appellant in the current case had been convicted of a drink driving offence in 2008.

62. The majority of the Supreme Court considered that it did not have to take the same approach as the Grand Chamber in *S v UK* (2009) 48 E.H.R.R. 50 in relation to the retention of biometric data of those who had not been convicted of an offence, when deciding whether there had been an unjustified breach of Article 8. The principles of proportionality whereby the Court in *S* had considered a number of factors (seriousness of the offence, age of the offender, time passed since offence committed) were not to be applied in the same way where a person had been convicted. It was noted that the retention scheme only applied to adults, and that the interference with the right to respect to private life would be small. There were considerable benefits to the police in retaining the information. Indefinite retention of the material was well within the margin of appreciation of the police in the circumstances.

63. Lord Kerr delivered a powerful dissent: he was firmly of the view that the *S v UK* approach should apply to convicted cases as well, and that a lawful system would require deletion of information when a conviction was deemed to be spent.

R (P & A) v Secretary State for Justice and others [2016] EWHC 89 (Admin)

64. The claimants challenged the amendments made to the criminal records disclosure scheme following the Supreme Court case of *R (T and B) v Chief Constable of Greater Manchester and others* [2015] AC 49. Amendments still contained provision for indefinite disclosure wherever a person had more than one conviction. Further, for certain professions similar changes were made to the rehabilitation of offenders legislation, but still exempted those with more than one conviction. Both the claimants had more than one conviction in the distant

past, for fairly minor matters. They sought declarations that the changes to the Police Act 1997 Part 5 and to the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 were incompatible with their right to respect for private life under Article 8 ECHR.

65. The Court found that the revised provisions did breach the claimants' Article 8 rights. The judgment concentrated on whether the revised scheme was "in accordance with the law" for the purposes of Article 8(2), rather than whether the scheme was justified and proportionate for a legitimate aim. The Court noted that the Supreme Court decision in *T and B* had changed the understanding as to how the "in accordance with the law" requirement should be applied (the Supreme Court had found that the original scheme was not in accordance with the law as well as disproportionate). The test to be applied was whether the revised scheme protected against arbitrariness, and whether there were sufficient safeguards for persons such as the claimants. The Court said that a scheme which could catch both the claimants and require indefinite disclosure of their convictions did not meet these tests and so the revised scheme was not in accordance with the law.