Clarifying the scope of personal data

In this tour of UK case law to date, Damien Welfare, Barrister at Cornerstone Chambers, discusses the challenges for organisations in interpreting the definition of 'personal data' in the UK, and considers the extent to which the new Regulation will provide greater certainty

Millions, if not billions, of pounds are being spent on data protection every year, by private companies and public bodies. In the UK, the Information Commissioner ('Commissioner') looms ever larger over issues such as data security, with the threat of substantial monetary penalties on data controllers. The news is full of stories about breaches of data protection rights. Yet at the heart of all this activity and enforcement lies an inconvenient fact: there is no settled understanding in the UK of the definition of personal data.

The definition of personal data in the UK is set out in Section 1 of the Data Protection Act 1998 ('DPA') and the Commissioner, the courts, the First-Tier Tribunal (Information Rights) ('the Tribunal'), the Upper-Tier Tribunal and practitioners have done their best to apply it, though not always in the same way. The Court of Appeal took a famously narrow approach in *Durant v Financial Services Authority* in 2003 that has placed the scope of the UK law out of step with other European countries. The House of Lords was obliged to try to make sense of the statutory definition in the context of anonymous data in the 2008 case of *Scottish Information Commissioner v Common Services Agency*; a decision whose interpretation occasioned further differences of view in the Tribunal, until it was helpfully interpreted by the High Court last year in *Department of Health v Information Commissioner.*

Yet still the uncertainty persists. Apart from the restrictive effect of *Durant*, there exists a mismatch between the definition in the DPA and that in the European Directive (95/46/EC) to which the UK legislation is supposed to give effect.

Thankfully, help may be at hand in relation to both problems, in the form of the proposed Data Protection Regulation. If enacted in its present form, the new Regulation will repeat and extend the definition in the Directive, but make it directly applicable in all Member States. The definition in the DPA will be repealed, and the caselaw on it will become out of date. However, until the new Regulation is both agreed and then implemented, which it is suggested may take as many as four years, organisations which carry out data processing in the UK must continue to persist with the existing definition.

Restrictive interpretation applied by Court of Appeal

The first problem in applying the definition of personal data arises not from the wording of the UK statute, but from the restrictive interpretation applied by the Court of Appeal to the overall concept.

In *Durant*, Lord Justice Auld found that the scope of 'personal data' should be limited in any particular instance to where it fell 'in a continuum of relevance or proximity to the data subject'. He suggested that two notions might assist in determining this: first, whether 'the information is biographical in a significant sense', so as to exclude 'a life event in respect of which his privacy could not be said to be compromised'; or, second, whether the information had 'the putative data subject as its focus'. In short, an individual's personal data was 'information that affects his privacy' (paragraph 28 of the judgment).

The decision caused consternation amongst practitioners by applying a far narrower interpretation to the definition of personal data than had developed as the norm. That said, it may be the case (as was hinted at by a judge in the *CSA* case discussed below), that the decision can be read as applying only in the context of subject access requests. The Court of Appeal did not accept that a very wide interpretation should be placed on the scope of a subject access request.

Also in this case, the court applied a restrictive interpretation to the meaning of 'data' in a 'relevant filing system', thereby further limiting the scope of personal data.

In response to *Durant,* the Commissioner revised his guidance on the definition of personal data (www.pdpjournals.com/docs/88015) (the 'Guidance'). The Guidance set out the scope of the definition in the Directive as applied in other EU Member States, and drew on a review of the

(Continued on page 8)

(Continued from page 7)

definition by the Article 29 Working Party.

The Guidance, which remains current, pointed to a wider interpretation of the definition, including information from which something could be learnt, recorded or decided about an individual; or where the purpose of the processing was to inform or influence actions or decisions affecting an identifiable individual.

The Information Tribunal, and its successor the Information Rights Tribunal, have continued to refer to the *Durant* decision as binding upon them. However, practitioners have in effect tended to follow the wider definitions reflected in the Guidance, doubtless on the precautionary principle that since care is needed in handling of personal data, the rights of data subjects are more likely to be protected, and particularly breaches by the data controller avoided, if the wider definition is adopted.

In the recent (2012) case of *Efifiom Edem v Information Commissioner's Office* ('ICO'), the Tribunal applied *Durant* to find that the names of members of staff of the Financial Services Authority who had sent emails as part of internal discussions of the Appellant's case were not their personal data. This was deemed to be the case because the emails were not biographical, nor were they the focus of the information, such that disclosure would not affect the individuals' privacy. Since they were not personal data, no exemption applied under section 40(2) of the Freedom of Information Act 2000, and their disclosure was ordered.

Unfortunately, the House of Lords took the view in the *CSA* case (discussed below) that the decision in *Durant* was not relevant to the matter before it, and therefore did not rule on whether its interpretation of the scope of personal data had been correct. A clarification of the present definition in a suitable case by the Court of Appeal, or the Supreme Court, would doubtless assist data controllers in general.

Wording of the DPA

The second problem arises from the wording of the DPA. Section 1(1) says that personal data means 'data' (i.e. information in the forms defined in the Act) that 'relate to a living individual who can be identified either from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'.

The definition goes on to make it clear that this includes expressions of opinion about an individual, or indications of intention towards them.

This part of the definition has not been problematic. The problem arises from the wording in the second part of the definition which introduces 'other information' into the definition, where that information is in the hands of the data controller (or likely to come into their hands). The wording leaves unclear what the data and the 'other information' should respectively comprise, how they should be combined and with what result; and whether it was the outcome of their combination that would amount to personal data (assuming that an individual could be identified from it), or both elements separately. We shall see below some of the contortions to which this part of the definition has given rise.

There is no reference to combining data with 'other information' in the Directive. Article 2(a) reads: 'for the purposes of this Directive: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

Recital 26 of the Directive gives a slightly greater basis for the UK approach, when it states: 'the principles of data protection must apply to any information concerning an identified or identifiable person; to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used, either by the controller or by any other person to identify the said person; the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. As can be seen, the test in the Directive is not concerned with information as such, or who holds it, but with any means reasonably likely to be used to identify the data subject. The view seems to have been taken by the drafters of the DPA that this test could fairly be interpreted to mean putting data together with other information in order to identify the person concerned. The Directive's intention was that the test should be whether any person, not merely the data controller, would be reasonably likely to be able to identify an individual. The limitation to information in the possession of the data controller (or that which he is likely to acquire) has no basis in the Directive, and has bedevilled the UK definition.

The difficulty caused by the UK limitation was for a while avoided as data controllers sought to rely on the Commissioner's Guidance. In Section D of the Annex to the Guidance, the Commissioner outlines the problem of a public authority responding to an FOI request for the home addresses of its staff, where the information sought does not directly identify individuals.

The Guidance states that 'they [public authorities] are nevertheless disclosing personal data if there is a reasonable chance that those who may receive the data will be able to identify particular individuals. The Guidance points directly to the issue that the DPA refers to identification solely by the data controller, so that releasing staff addresses might appear not to be disclosing personal data, but contrasts this with the definition in the Directive. The Guidance advises data controllers to adopt a purposive interpretation, and refers to the decision of the Information Tribunal in *Colin England v LB Bexley and Information Commissioner's Office* (2006) in which the Tribunal held that releasing the addresses of empty properties would involve releasing personal data where the properties were owned by individuals.

On occasions where the question of the scope of personal data arises in

practice, and particularly in relation to FOI requests involving personal data, the judgment appears often more likely to be focussed on whether the recipient could identify an individual from the information in question, rather than on what other information the data controller might or might not be able to put alongside that information.

This issue was addressed again directly by the House of Lords in the context of anonymous data in *CSA.* The request was for data concerning incidents of leukaemia in children by year and census ward in a postal area. It was unclear whether the data had been rendered anonymous by a technique known as 'Barnardisation', and the issue was whether these data amounted to personal data under the DPA.

Illustrating the difficulties of the definition, the five judges were split four ways on how to interpret it, and particularly the second part of the definition. Only one other judge wholly supported the leading judgment. (One of those who took a different view from the leading judgment supported it if his own approach were not correct and another preferred it to that of his colleague, without deciding between them).

Whether or not the data were anonymised to the potential recipient, it was evident that since the Agency still held the original information from which it had derived the statistics, it could still identify the children concerned. The issue was whether this would bring the data (if anonymised) within the second part of the definition, such that any publication would have to conform to the requirements of the DPA. Lord Hope held that it would not, provided the data were fully anonymised, since both the anonymised data and the other information had to contribute to the identification, in order for the former to constitute personal data under the second part.

> ***"What matters is that disclosures that potentially affect privacy are regulated according to the Data Protection Principles, and that the test of whether those Principles potentially apply should be determined in the first instance by whether any means are reasonably likely to be used by any person (including, but not limited to, the data controller) to identify the individual. The introduction of the Regulation, if enacted in this form, will require data controllers in the UK to move to this test."***

Mr Justice Cranston later said in *the Queen on the application of Department of Health v ICO* (2011) that "it would be wrong to pretend that the interpretation of the *CSA* case is an easy matter". In the Tribunal in the same case (*Department of Health v ICO and Pro Life Alliance*), both parties sought to rely on Lord Hope's reasoning. The request was for annual statistics on certain types of abortions.

On the question whether the statistics were personal data, the Commissioner argued that the issue was whether they would be anonymous to a third party (i.e. effectively, whether individuals could be identified by a recipient). If they could not be so identified, they would not be personal data.

However, the Tribunal took the view that the *CSA* case had decided that anonymisation would only place data outside the DPA if they could not be reconstituted into their original form by the Agency. Otherwise, the statistics would in its view remain personal data.

In *Magherafelt District Council v ICO* (2009), both parties again relied on the *CSA* case. The Tribunal took the same approach as in the *Department of Health* case on the question of the circumstances in which anonymised data would no longer be personal data.

Further differences of view emerged in the decision of the Upper-Tier Tribunal in *All Party Parliamentary Group on Extraordinary Rendition v ICO* (2011). In that case, the Tribunal decided that, given the disparity of the judgments in the *CSA* case, it was open to it to adopt the pragmatic minority view of one of the judges in that case. That view was that fully anonymised data remains personal data in the hands of the data controller, who must observe the Data Protection Principles in processing it internally (as long as he can continue to identify the individuals involved). However, such data ceases to be personal data in the hands of the recipient, because the public cannot identify any individual from it.

The appeal from the decision of the Tribunal to the High Court in the *Department of Health* case concerned whether statistics concerning late term abortions should continue to be published. The Department of Health argued that disclosure would create a real risk of patients being identifiable. Certain categories had been combined and cell counts below 10 suppressed for any single year, but aggregated over three years. The Commissioner and Tribunal had both ordered disclosure, though the Tribunal considered that the statistics were personal data, whereas the Commissioner did not.

The judge said that Lord Hope's judgment in the *CSA* case did not mean that, given that the Agency had held the original information, the data that derived from that information (and

(Continued on page 10)

(Continued from page 9)

thus with which it could be combined) were personal data. If that were the correct interpretation, he said, any publication of a simple total number from statistics would be the personal data of all those whose cases were included within the figures; a situation he considered to be "divorced from reality".

It was the judge's view that the correct interpretation of Lord Hope's judgment must be that where the statistics were truly anonymised, so that no information about a person could be derived from them alone, the statistics would not be personal information when disclosed. Both the statistics and the 'other information' thus had to add something to the mix, in order for the statistics to count as personal data under the second part of the definition in the DPA. If the data on their own added nothing because of the degree of anonymisation, they would not be personal data.

Although greater clarity appears to have been achieved as to the meaning of the second part of the DPA and how it should be applied, the position is still unsatisfactory.

The new Regulation

Article 4(2) of the new Regulation defines 'personal data' simply as 'any information relating to a data subject'. Article 4(1) defines a 'data subject' as: 'an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person'.

As can be seen, the scope and concept of the definition are broadly similar to that in the present Directive. (The differences are in the Regulation's expression of the core of the definition in relation to the data subject, rather than to personal data; the addition of areas such as 'genetic data' to the definition (and the creation of a separate category of 'health data'); and the references to some recent technological developments such as online identifiers.)

Recital 23 is phrased in similar terms (save that, like the existing Recital 26 of the Directive, it refers to means 'likely reasonably' to be used, rather than means 'reasonably likely' so to be used, a point picked up by the ICO in its response to the draft).

The difficulties with the second part of the definition are essentially very straightforward, notwithstanding the debate they have engendered. If data on their own (e.g. an isolated fact about a service complaint to a company) cannot realistically be related to any individual in the hands of a recipient, but can be so related in the hands of the data controller because of other information he holds (such as the file on the complaint), it seems paradoxical to apply the rigour of data protection to disclosure of the isolated fact.

On the other hand, if the recipient is likely to have access to some knowledge that would enable him to identify the individual from the isolated fact (e.g. by access to the employee complained about), it would seem to be contrary to the presumed purpose of data protection law to ignore that factor and to declare disclosure to fall outside the data protection regime, merely because the further information is held by someone other than the data controller.

What matters in both cases is that disclosures that potentially affect privacy are regulated according to the Data Protection Principles, and that the test of whether those Principles potentially apply should be determined in the first instance by whether any means are reasonably likely to be used by any person (including, but not limited to, the data controller) to identify the individual. This was the position set out in the Directive and is substantially repeated in the new Regulation. The introduction of the Regulation, if enacted in this form, will require data controllers in the UK to move to this test.

Only on that basis will the widest practicable level of protection of personal information — including of information that is reasonably likely to be combined with other information or knowledge, to produce data about an individual that is deserving of protection — be achieved. At the same time, the net of data protection should not be cast so wide that harmless facts or statistics could be rendered incapable of disclosure. This requires, in terms of the definition of personal data, a practical interpretation of the scope of the means reasonably likely to be used to identify an individual.

Finding the balance between these two objectives will doubtless form one of the key challenges in implementing the new Regulation. The hope is that, with the complication of the UK limitation removed, it will be possible to evolve an approach in the UK that borrows more from experience in other Member States, and that is more in step with those implementing the same legislation elsewhere in the EU.

Damien Welfare
Cornerstone Barristers
damienw@cornerstonebarristers.com