SCRIPT-ed

Volume 1, Issue 2, June 2004

Taking the "Personal" Out of Personal Data: *Durant v FSA* and its Impact on the Legal Regulation of CCTV

Lilian Edwards[*]

DOI: 10.2966/scrip.010204.341

[*] Co-Director, AHRB centre for IP and Technology Law, Edinburgh School of Law, l.edwards@ed.ac.uk.

What is "personal data" for the purposes of European and UK data protection (DP) legislation? Since European DP law controls only the automatic or partially automatic processing of "personal data" relating to "data subjects", how this phrase is defined is a crucial step in ascertaining how wide the protection of DP law really is, and to what extent it safeguards personal privacy in the information society. To date, somewhat surprisingly, there has been relatively little judicial guidance in UK law or in the European Court of Justice on this point[1]. Now however the scope of "personal data" has been narrowed in the UK at least by the controversial Court of Appeal decision in *Durant v FSA*[2]. Although the case itself is about disclosure of information in the financial services sector, somewhat unpredictably the main impact of *Durant* has been in what at first blush seems to be a remotely connected area, that of the field of legal regulation of closed circuit TV cameras (CCTV)[3]. This note will focus on that domain.

Section 1(1) of the Data Protection Act 1998, implementing Art 2(a) of the EC Data Protection Directive 1995[4], defines "personal data" as

> "*data which relate to a living individual who can be identified*
>
> *a) from those data, or*
>
> *b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller…." [italics added]*

Until recently, a wide definition of "personal data", tailored to fulfil the purposes of the DP legislation – namely to protect personal privacy – was anticipated by most commentators. However in the first UK case to grapple in detail with this issue, *Durant v FSA*[5], this assumed wide interpretation of "personal data" was unexpectedly narrowed by the English Court of Appeal. The plaintiff Durant was in dispute with Barclays Bank, and made a complaint to the Financial Services Authority (FSA) about their behaviour, which lead to a confidential inquiry by the FSA into the bank's conduct. Durant, having already failed in various law suits against Barclays, now sought sight of all records held by the FSA which mentioned his name or in were in any way "related to" him, on the grounds that they were "personal data" of which he was the subject and to which, by ss 7(1) and 8(2) of the 1998 Act, he thus had rights

---

[1] The recent ECJ case of *Lindqvist* ECJ, Case C-101/01, 6 November 2003 does touch on the issue of what is personal data, in relation to textual information uploaded to the Internet, but has little that is incisive on this point, and is rather more significant on the definitions discussed therein of both "automatic processing" and "transfer to third country". Basically all that is said about personal data is that it definitely includes "the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies" (ibid, paras 25, 27). An interesting contrast is the recent Icelandic Supreme Court decision in the albeit very different context of genetic/health data, *Gudmundsdottir v Iceland*, November 27 2004, which by contrast to *Durant* widens rather than narrows the national interpretation of "personal data".

[2] 2003] EWCA Civ 1746

[3] See also Rowe H "CCTV Systems and the Data Protection Act 1998" (2004) 20 (3) CLSR 221. *Durant* lead directly to special guidance appearing as fast as possible on the Information Commissioner's website amending the already existing CCTV Code of Practice: see http://www.informationcommissioner.gov.uk/cms/DocumentUploads/CCTV%20additional%20guide.pdf .

[4] 95/46/EC.

[5] Supra n 3.

of access. The focus of *Durant* was thus primarily on how widely the phrase "relate to" in s 1(1) should be interpreted, so as to determine what information Durant had a right to see. This was an unexpected line of enquiry, as most academic commentary before that case had largely anticipated dispute only about the meaning of the phrase "identified"[6].

A second area of dispute in *Durant* concerned redaction. Durant had already been given sight of some records by the FSA which had been "redacted" ie, had had the names of parties other than himself masked out so as to preserve their rights of privacy. DP law recognises that the privacy rights of third parties mentioned incidentally in records must be preserved notwithstanding the rights of subject access granted to data subjects. A balance is set up in s 7(4)(b) of the 1998 Act whereby if a data controller cannot comply with the request in hand without disclosing information identifying another individual, he is not obliged to comply with the request unless *either* that other individual consents *or* it seems reasonable to comply with the request without that consent. The question in *Durant* was whether Durant had a right to insist on seeing the un-redacted originals.[7].

On the first point as to the width of the phrase "relate to", two interpretations were quoted from the Shorter Oxford Dictionary: a narrower definition which said it meant "having reference to, concern" ; and a wider definition , namely, "having some connection with, be connected to". Auld J, giving the lead opinion of the court, preferred the more restrictive definition. This was, he claimed, more in accordance with the purposes of the EC DP Directive, which were to give the data subject access to "information about himself" and not to specific documents *per se*. Section 7 of the 1998 Act, which implemented that part of the Directive in the UK, similarly was not intended to be an "automatic key to information", nor to allow access to any and all documents mentioning the data subject's name, nor, importantly, any and all which might be retrieved by putting the subject's name into a search engine. Instead, the aim of the data subject access rights was merely to enable the subject to protect *his privacy* by finding out what the data controller held about him, and whether the processing of that data unlawfully infringed DP law.

Auld J, having effectively narrowed the definition of "personal data", then gave two examples of what types of information *would* now be subject to DP protection. "Mere mention of the data subject in a document held by a data controller," would not, he opined, "necessarily amount to his personal data." Whether any particular information amounted to "personal data" would in general depend on where it fell in a "continuum of relevance or proximity" to the data subject. However, for guidance, if information was "biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or event that has no personal connotations" then it was likely to be regarded as "personal data" [8].

---

[6] See Jay R. and Hamilton A. *Data Protection Law and Practice* (2nd edn, 1999, Sweet and Maxwell); Carey P., *Data Protection: A Practical Guide to UK and EU Law* (Oxford University Press, 2nd edn, 2004) pp14-15; Edwards L. "Canning the Spam" in Edwards L. and Waelde C. eds. *Law and the Internet: A Framework for Electronic Commerce* (Hart Publishing, 2000), pp 320-321 (on whether email addresses constitute personal data).

[7] A third point discussed at length in *Durant* related to the definition of manual filing systems for DP purposes: however this is not relevant to the topic of personal data and CCTV regulation and so is here omitted.

[8] *Durant v FSA*, supra n 3, para 28.

Secondly, the matter of "focus" needed to be taken into account.

> *"The information should have the data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or had an interest… In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity."*[9]

Accordingly in the case at hand, many or most of the records Durant sought, which bore his name as the complainant and which would be found if Durant's name was used as a search term, but which fundamentally related to Barclay's Bank rather than containing "biographical details" about Durant, or with a "focus" on Durant, were no longer to be regarded as "personal data" relating to Durant, and thus he had no rights as data subject to request access to those records.

On the redaction issue, the issue was largely a dead one by this stage as so much of what Durant was seeking access to was no longer defined as his "personal data". Accordingly, Auld J merely noted, first, that if the identifiable references to other individuals contained in a record were not "personal data" relating to the applicant under the new, narrower interpretation, then no balancing act need be done under s 7(4) at all , ie, there was no need to decide if it was "reasonable" to release the information to the applicant (and thus blanket redaction would in many cases be justified) . Secondly, Auld J noted that even if references did constitute the "personal data" of *both* the applicant *and* another data subject, the data controller was not required to go through a first step of seeking the consent of that other person if it *was* reasonable to release the information. Thirdly, in deciding what was "reasonable", a data controller should take into account the "legitimate interest" (if any) the data subject had in requesting the disclosure of the identity of another identifiable third party individual; and the degree to which the third party information necessarily formed part of the data subject's *own* personal data to which access was sought. These last two factors were unlikely to come into conflict, as it would be "difficult to think" of a case where third party information was so bound up with the applicant as to constitute "personal data" relating to the applicant and yet the applicant had no legitimate aim in obtaining that third party data.

Durant is a very understandable decision on its own facts. The Court of Appeal was stuck between the rock of data protection and the hard place of forcing a data controller like the FSA to effectively give access to all its confidential records to an individual who might abuse that access, and at the expense of its own external relationships with the community it regulates. The FSA is a regulatory body whose efficiency is (or was) based on being able to investigate financial organisations on a basis of confidentiality (it should be noted this case preceded the coming into force of relevant freedom of information legislation). Durant was, in essence, it seems, seeking not so much traditional data subject access rights, as rights of freedom of information in relation to the FSA investigation which UK law simply did not give him at the time. He was also seeking a last bite at the cherry having failed to see Barclay's Bank punished both in his own litigation and during the FSA investigation. It is clear the court felt he was more interested in finding out "personal data" about others rather than himself, with a view to more litigation, not protecting his own privacy – a fundamental misconception of what DP law is meant to do – hence, no doubt, the

---

[9] Ibid.

repeated emphasis in the opinion on the purpose of the DP Directive being to protect the data subject's own *privacy*.

But, perhaps unexpectedly, since the dust settled on Durant it has become apparent that its main impact is not on the domain of financial services (which is in any case now gearing itself up to provide publication schemes to meet with the new freedom of information requirements) but in the context of CCTV and data subjects whose images are captured on CCTV. Here, *Durant* unexpectedly ushers in a major change in the law and one which may well jeopardise the legitimate expectations of privacy of UK citizens and employees, and be out of step with the rest of the European DP community. Indeed, several commentators have suggested that the *Durant* decision should have been referred to the ECJ to provide a harmonised EC response[10].

Before *Durant*, when it was assumed that "personal data" would be given a relatively wide, non-technical interpretation, it appeared that CCTV images captured of living individuals would be subsumed under "personal data" so long as an individual who could be identified was depicted on-screen. This wide interpretation of personal data had the *prima facie* consequence that all operators of CCTV schemes however basic needed to notify with the Information Commissioner as data controllers and that all identifiable CCTV images were subject to the full DP requirements of fair processing (subject, of course, to exceptions such as those intended to promote law enforcement and national security[11], and to promote freedom of expression[12]). Only pictures of people who could not be identified would fall outside the scope of the DP regime, and, even then, not if they could be identified if cross-referenced with other data the data processor had, or was likely to have : for example, images in stadiums or cinemas can be cross matched with seat records; shops can match images of customers paying with names on credit cards or store cards they used during the transaction[13].

After *Durant*, however, the scope of what falls within DP regulation in terms of CCTV suddenly looks very different. The Information Commissioner has speedily issued detailed guidance on what the narrowing of the definition of "personal data", and the two new guidelines as to "biographical" data, and "focus" mean in the context of CCTV[14]. The new guidance advises:

---

[10] See Chalton S. "Reflections on *Durant v FSA*: The Court of Appeals' interpretation of "personal data" in *Durant v FSA* – a welcome clarification or a cat among the data protection pigeons?" (2004) 20(3) CLSR 175; editor's opinion of Mason's Out-LAW Reports at http://www.outlaw.com, 19-5-2004.

[11] See ss 28 and 29, 1998 Act.

[12] See s 32, 1998 Act. But note that the exemption of journalists from seven of the Eight DP principles (data security is still required) is limited by a "public interest" test: s 32(b). It is an open question if it could ever be in the "public interest" for a journalist to train a CCTV camera on the door of (say) a celebrity's home or place of work night and day – the result at the High Court stage in *Campbell v MGM* [2002] EWHC 499 (QB), where an award of damages for breach of DP rights, albeit nominal, was made to Ms Campbell in similar circumstances involving mere "still" press photographs, as opposed to CCTV, would seem to indicate not..

[13] See Carey P, supra n 6, Chapter 15: CCTV.

[14] See http://www.informationcommissioner.gov.uk/cms/DocumentUploads/CCTV%20additional%20guide.pdf .

> *"…If you have just a basic CCTV system, your use may no longer be covered by the DPA. This depends on what happens in practice. For example, small retailers would not be covered who:*
>
> - *only have a couple cameras,*
> - *can't move them remotely,*
> - *just record on video tape whatever the cameras pick up, and*
> - *only give the recorded images to the police to investigate an incident in their shop."*

The shopkeepers would need to make sure that they do not use the images for their own purposes such as checking whether a member of staff is doing their job properly, because if they did, then that person would be the focus of attention and they would be trying to learn things about them so the use would then be covered by the DPA.

It sounds like many users of basic CCTV systems are not covered by the DPA, is there an easy way to tell?

Think about what you are trying to achieve by using CCTV. Is it there for you to learn about individuals' activities for your own business purposes (such as monitoring a member of staff giving concern)? If so, then it will still be covered. However if you can answer 'no' to all the following 3 questions you will not be covered:

- Do you ever operate the cameras remotely in order to zoom in/out or point in different directions to pick up what particular people are doing?
- Do you ever use the images to try to observe someone's behaviour for your own business purposes such as monitoring staff members?
- Do you ever give the recorded images to anyone other than a law enforcement body such as the police?"

As can be seen from the above, the Information Commissioner seems to be taking the approach that if a simple CCTV system is not intended to (or is not physically able to) "focus" on any given individual, nor is intended to provide specific intelligence of a "biographical" nature about a particular person (for example, follow a suspect employee around) then it is not collecting "personal data relating to" any person at all, despite the fact that images of living identifiable persons *are , in fact,* captured. And since no personal data is collected, there is no need to respect the rules of data protection, nor for the system operator to notify the Information Commissioner as a data controller. The CCTV system, it seems, entirely drops out of the DP net.

What about more sophisticated systems? The guidance continues:

> *"In many CCTV schemes, such as are used in town centres or by large retailers, CCTV systems are more sophisticated. They are used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness or assessing how an employee is performing. These*

> *activities will still be covered by the DPA but some of the images they record will no longer be covered. So if only a general scene is recorded without any incident occurring and with no focus on any particular individual's activities, these images are not covered by the DPA. In short, organisations using CCTV for anything other than the most basic of surveillance will have to comply with the DPA but not all their images will be covered in all circumstances. The simple rule of thumb is that you need to decide whether the image you have taken is aimed at learning about a particular person's activities." [italics added]*

This leaves open the possibility that although a CCTV system of a certain complexity may "qualify" for the DP regime – with the result that the CCTV operator will need, for example, to notify the Information Commissioner as to the purposes for which he is collecting the data - the images of persons which are collected incidentally, without "focus", will not be regarded as "personal data". This mean the key obligations DP imposes *from the point of collection*, such as fair processing, data security and no unreasonable data retention, disappear. Furthermore, persons whose images are so incidentally collected, and which are thus not categorised as their "personal data", will have no rights to access or correct these images under subject access rules, nor, perhaps, to control how they are processed. They will have in principle, it seems, no right to demand that those images be "redacted" – in this context, edited out or masked or pixellated into obscurity – if a tape on which they feature incidentally is given to another data subject featured therein - as, extending the dictum of Auld J, the "reasonableness test" under s 7(4) of the 1998 Act, which requires the data controller to balance the access rights of the applicant data subject against the privacy rights of any other party whose personal details are disclosed, will not cut in if those details are not deemed "personal data" of the third party captured[15]. (And since editing is an expensive process which many CCTV controllers will need to contract out and pay for, a simple request, un-backed by law, is unlikely to cut any ice.)

In essence, the degree to which these CCTV images are part of the personal private sphere of the individual identifiable therein, has ceased to be the focus of the law's concern; what will really matter, in practical terms, is the intentions and goals of the CCTV *operator* when he or she sets up the cameras, and how this is translated into the physical set up and management routine of the system. This has potentially staggering implications in the CCTV field. What if the London Congestion Charging Authority – whose CCTV cameras are primarily intended to track license plates so as to identify who should be paying the toll - incidentally collect images of semi-famous celebrities in potentially embarrassing situations (eg, badly dressed or with unstyled hair)? Leaving aside issues of common law privacy (see below), in DP terms it seems these pictures might well not be "personal data" at all, because the celebrity would not have been the "focus" of the system nor does the picture tell you anything very "biographical" about him or her. Their presence is incidental to the data collector's notified purposes. Accordingly the DP regime would not apply at the point of collection. The London Congestion Charging Authority's notification says nothing about one of the purposes of their data collection activities being to collect pictures which might one day make their unwanted way to paparrazi – but it would become a

---

[15] *Duran v FSA*, supra n 3, para 55.

possibility, with no breach of the First Data Protection principle which requires that methods of collection of data be "fair". What then happens to the "reasonable expectations" and privacy rights of the millions (including but not limited to celebrities) who journey into central London by car every day in reach of the camera eyes?

Of course it could be argued that once an incidental image captured of – say – Kylie Minogue, had been discovered *and* offered to the *Daily Mail* for a four-figure sum, that data now would certainly *become* "personal data" relating to, and identifying, Ms Minogue, and thus the processing of it, in the form of distribution or sale, would be controlled by DP law, which would spring into action as a relevant legal regime. Indeed this seems to be the interpretation favoured by the Information Commissioner, since in the guidance notes quoted above, the third question the operator of a small CCTV system must ask to know if he or she still needs to notify under DP law post-*Durant*, is "Do you ever give the recorded images to anyone other than a law enforcement body such as the police?".

However although this interpretation – the idea that CCTV images might not be "personal data" at the moment of collection but could be retrospectively constructed as such - is possible it is (a) still not very satisfactory as requirements of fair processing should operate from the moment of collection, not *post hoc*, and (b) though not ruled out by *Durant*, does not seem on close scrutiny to be backed by it either. Auld J's opinion seems impliedly limited to requiring an assessment of whether information is to be categorised as "personal data" (or not) at the time when the data subject access application is made, based on the history of the information to date[16]. There is no reference to any factors which might turn non-"personal data" into protected data in the hands of a data controller at some later date. One would hope that such an interpretation would however recommend itself to a later court: especially given the second clause of the definition of personal data in s 1(1) of the 1998 Act, which clearly contemplates future events being relevant to the classification of information as personal data (data may become personal data when combined with "other information which is in the possession of, *or is likely to come into the possession of,* the data controller") [italics added]. Any other approach would also apparently breach Art 8 of the European Convention on Human Rights (ECHR) as it would mean there was no legal remedy in UK courts for a breach of the Art 8 right to respect for private life, as upheld in *Peck v UK*[17].

It seems likely that *Durant* as a whole may soon hopefully appear before the European Court of Justice for review[18]. At that stage, this commentator would hope for a different outcome, which respects the basic principle that personal privacy as a policy goal in the DP framework, should lead to a primary focus on the rights of the data subject whose image is captured, not on the procedures and administrative overhead of the data controller who captures the image. The impact of *Durant* on legal regulation of CCTV is particularly important in the UK, which, to most people's ignorance and lack of concern, is well on the way to becoming the "surveillance society" of Big Brother bad dreams: not because of the much trumpeted menace of ID

---

[16]Ibid, paras 24-31.
[17] (2003) ECHR Application No. 44647/98.
[18] http://www.outlaw.com , 19-05-2994, reported that Durant had filed papers with the European Commission claiming the UK government has not implemented the Data Protection Directive correctly.

cards but because of the so ubiquitous as almost to be invisible pervasive growth of semi covert surveillance by CCTV. The *Independent* newspaper has estimated that over 4 million cameras are being used in the UK, 20% of all the CCTV cameras in use in the world, and that the average Briton is caught on camera 300 times a day[19]. Such blanket CCTV coverage has, it is claimed, many conspicuous benefits in terms of crime detection, prevention and prosecution, and the building of public trust. However in a world of such singular Panopticism, it is vitally important that the principal legal control over CCTV which data subjects have – data protection law – should not be interpreted in a way which diminishes its value to the non-criminal citizen who is merely seeking to protect their privacy, as is their inalienable human right.

[19] http://news.independent.co.uk/uk/this_britain/story.jsp?story=480364 .