CIRL374426

Queries

Karen McCullagh

Dear Author
Please address all the numbered queries on this page which are clearly identified on the proof for your convenience.

Thank you for your cooperation

Q1 Please supply affiliation address.

Q2 Words such as "current" and "recently" are problematic as they depend on date written/being read. Please qualify by adding date or substitute actual dates/specific periods as necessary or use "at time of writing **date**", for example.

Q3 Please provide last accessed dates for web addresses.

Q4 Is this note OK?

Q5 Note OK as changed?

Q6 Please provide more detail for this note and last accesed date.

International Review of Law, Computers & Technology
Vol. 23, Nos. 1–2, March–July 2009, 47–58

Routledge
Taylor & Francis Group

Protecting 'privacy' through control of 'personal' data collection: a flawed approach

Karen McCullagh* Q1

The development of a frontier-free internal market and of the so-called 'information society' have resulted in an increase in the flow of personal data between EU member states. To remove potential obstacles to such transfers, data protection legislation was introduced. One of the underpinning principles of Directive 95/46/EC is the protection of privacy. Yet, the legislation does not provide a conclusive understanding of the terms 'privacy' or 'private' data. Rather, privacy protection is to be achieved through the regulation of the conditions under which personal data may be processed. An assessment of whether, 10 years after the enactment of the Data Protection Act 1998 (DPA 1998), a coherent understanding of the concept of personal data exists, necessitated an analysis of the decisions in *Durant* v. *FSA* ([2003] EWCA Civ 1746) and *CSA* v. *SIC* ([2008] 1 WLR 1550, [2008] UKHL 47). Furthermore, in order to examine the effectiveness of the current legislative model, this article examines whether the term 'personal' is synonymous with the term 'private' data and whether control over processing of personal information protects privacy. By drawing on interviews with privacy and data protection experts, and from the findings of a survey of bloggers, it will be shown that a review of the assumptions and concepts underpinning the current legislation is necessary. Q2 Q2

Keywords: data protection; personal; private

Introduction

As IT usage and processing capabilities evolve, regulators, privacy practitioners and citizens are increasingly questioning the suitability and adequacy of the current data protection legislation to allow the effective processing of personal data while simultaneously safeguarding the privacy of individuals. Indeed, the Office of the UK's Information Commissioner (ICO) recently commissioned research into how the EU Directive should be updated, because Q2 Q2

> We want to generate new thinking. European data protection law is increasingly seen as out of date, bureaucratic and excessively prescriptive. It is showing its age and is failing to meet new challenges to privacy, such as the transfer of personal details across international borders and the huge growth in personal information online.[1]

This article begins by exploring the relationship between privacy and data protection at EU and UK level. It will be demonstrated that the concepts of 'privacy' and 'private' data remain nebulous as they are not defined in the Directive. Instead, the Directive provides a definition of 'personal' data and stipulates the conditions under which such data may

*Email: k.mccullagh@salford.ac.uk

ISSN 1360-0869 print/ISSN 1364-6885 online

DOI: 10.1080/13600860902742562
http://www.informaworld.com

be processed. Thus, this research explores the meaning of the term 'personal' data by reviewing the cases of *Durant* v. *FSA*[2] and *CSA* v. *SIC*.[3] Also, the article assesses whether control over personal information protects privacy by drawing on interviews with privacy and data protection experts from a range of countries and disciplines. Furthermore, the views of potential data subjects are explored through a survey of bloggers, which reports their conceptions of the terms 'private' data. The article concludes that a review of the current legislation is necessary, and that, in particular, the assumptions and concepts underpinning the term 'personal' and 'private' need to be revised. **Q2**

Privacy in Directive 95/46/EC

The goal of privacy protection is expressly stated in the opening provisions EU Directive 95/46/EC, wherein Art. 1 states that the objective is:

> to protect the fundamental rights and freedoms of natural persons and in particular their right to *privacy*, with regard to the processing of personal data. (Emphasis added)

However, the term privacy is not defined in the Directive. Rather, the Directive seeks to achieve privacy protection through regulation of the processing of personal data. This is understandable because no adequate definition of privacy has ever been produced.[4]

Personal data defined

The Directive prohibits, subject to exhaustively listed exceptions, the collection and processing of personal data. In the DPD, personal data is defined in Art. 2 (a) as:

> Any information relating to an identified or identifiable natural person; 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, psychological, mental, economic, cultural or social identity.

Whereas, personal data is defined in the Data Protection Act 1998, 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, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Korff[5] noted that the DPA 1998 makes a formal distinction between 'data' and 'information' but that in practice, it produced no material differences. The definitions in the Act and Directive are consistent in their use of the phrase 'relate to' but, under the Directive, consideration is first directed to whether the information relates to an identifiable individual and then whether it is processed. Whereas, the definition of personal data in the Act approaches the concept in the reverse order, as the Act focuses on the issue from a processing view first and then moves on to whether or not there is an identifiable individual. The Directive and Act also differ with respect to when an individual should be considered as 'identifiable'.

The term is wider under the DPA as it includes information that 'may' come into the possession of the controller. Korff argues that the phrase may mean that the definition of personal data in the Directive can be read as being 'relative', because potentially 'any data that can conceivably be linked to an individual (in whatever way, by whoever) [can] be regarded as personal'.[6] Booth et al.[7] observed that the way that the phrase 'relate to' is interpreted has major implications regarding what is or is not classed as personal data. If it is interpreted very narrowly, the term personal data could be restricted to data which is capable of identifying an individual, either by itself or in combination with other data. Identification, in this context, could be direct or indirect. In contradistinction, if the term 'relating to' is interpreted broadly it could conceivably include any data which may 'affect' the individual in some way, regardless of its capacity to identify. The consequences of a narrow interpretation of 'relating to' will be explored in an analysis of the Durant decision.

UK interpretation of 'personal' data

In the case of *Durant* v. *FSA*,[8] Mr Durant had lodged a complaint with the Financial Services Authority following a legal dispute with Barclays bank. The FSA dismissed his complaint. He then made a subject access request for information held manually and electronically by the FSA on his complaint. The FSA released the information held in computerised form, but refused to disclose the information held on manual files. Mr Durant applied to the Court under s 7(9) of the DPA 1998 for an order requiring the FSA to comply with the subject access request. The Court of Appeal was asked to decide: was the information held by the FSA relating to the investigation of Mr Durant's complaint 'personal' data under the Data Protection Act 1998? The definitional issue which arose concerned whether the data could be said to 'relate to' Mr Durant.[9]

Mr Auld LJ referred to Directive 95/46/EC and ruled that the statutory right of access under the DPA is designed to enable the data subject to:

> check whether the data controller's processing of it unlawfully infringes his privacy and, if so, to take such steps as the Act provides . . . to protect it.[10]

From this the Court concluded that the relevant information is:

> information that affects [the data subject's] privacy, whether in his personal or family life, business or professional capacity.[11]

This interpretation of personal data means that not all identifying information will fall within the scope of 'personal' data. Rather, only information that is capable of adversely affecting the privacy of the data subject will be considered personal. In order to determine whether or not data 'relates to' the data subject, Auld LJ proposed two tests.The first test is:

> whether the information is *biographical* in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised.[12] (Emphasis added)

The second test is whether:

> the information has the putative *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 have had an interest, for example, . . . an investigation into the some other person's or body's conduct that he may have instigated.[13] (Emphasis added)

Buxton LJ agreed, stating that the potential effect of processing of particular data on an individual's privacy was the guiding principle. The Court also drew support for a narrow interpretation of the term personal data from the wording of the DPA 1998. Auld LJ asserted that the DPA's definition of personal data extends to expressions of opinion about an individual which would be otiose if the words 'relate to' were construed broadly. Thus, the Court of Appeal ruled that the information about Mr Durant's complaints to the FSA or about their investigation of his complaint were not 'personal data' as the data did not relate to Mr Durant in the requisite sense. Rather, the Court decided that the information sought by Mr Durant was information about his complaints, as opposed to data relating to him. Furthermore, the Court ruled that the mere fact that a document is retrievable by reference to the name of the data subject does not render the information personal data:

> Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject.[14]

Thus, simply because an individual's name appears on a document, the information contained in that document will not necessarily be personal data about the named individual. Rather, it is more likely that an individual's name will be 'personal data' where the name appears together with other information about the named individual such as address, telephone number[15] or information regarding his hobbies.[16]

This conception of the term personal data is very narrow. If this decision were to be followed, only information that is capable of adversely affecting the privacy of the data subject would be considered personal data. Subsequently the Art. 29 Working Group issued an opinion on the concept of personal data,[17] which contains a broader notion of personal data. Thereafter, the Office of the UK Information Commissioner issued a technical guidance note[18] to the effect that Durant is relevant to the question of whether data 'relates' to a living individual only in difficult cases where the information in question is not 'obviously about' someone. However, the ICO guidance note is not legally binding, as the Durant decision has not been overruled.

In the case of *CSA* v. *SIC*,[19] a researcher submitted a request under the Freedom of Information (Scotland) Act 2002 (or 'FOISA')[20] to the Common Services Agency (the 'CSA'),[21] for details of the recorded incidence of childhood leukaemia for certain years in a geographical area, broken down by census ward. The researcher wanted to explore a suspected risk to public health arising from the Ministry of Defence's operations, a decommissioned nuclear reactor and an operational nuclear processing facility. The CSA refused to disclose the information on the grounds that it was personal data, the disclosure of which would breach the data protection principles. On application to the Scottish Information Commissioner (the 'SIC'), the SIC ordered the CSA to disclose the information sought in an anonymised form using a technique called 'barnardisation' which perturbs the dataset in order to substantially reduce the risk that individual data subject could be identified from it. The case raised the importance of whether or not the barnardised information was 'personal data' within the meaning of the DPA 1998.

The Lords ruled that the barnardised data was information about the health of the children involved. It therefore obviously related to the children and there was therefore no need to turn to the Durant decision and its concepts of 'focus' and 'significant biographical data', to decide whether the definition of 'personal data' was satisfied.

The second issue which arose was whether any of the children could be identified from the barnardised information (either alone or taken together with other information in the possession, or likely to come into the possession, of the CSA). The Court unanimously ruled the fact that the CSA continued to hold 'other information' which would ultimately have allowed it to 'decode' the barnardised information to identify each of the children to whom it related, did not necessarily mean that the barnardised information was still personal data. However, several different rationales can be identified from the judgment.

Lord Hope took the view that data can be 'fully anonymised' in the hands of the data controller and thereby cease to be personal data, even where the data controller does have information which would theoretically allow it to unlock the identities of the subjects of that data, but did not explain exactly how, or, in what circumstances that anonymisation might be achieved. Lord Rodger thought that data would remain personal data in the hands of the data controller provided that the data controller could identify the subjects of that data using 'reasonable means'. However, the practical implications of that reasoning are not clear. In marked contrast, Baroness Hale focused instead on the proposed recipient of the data, and whether he or should could identify the subject(s) of that data from that data alone (given that he or she would not have access to any of the 'other information' in the hands of the disclosing data controller). This lack of unanimity appears to have arisen from the difficulty which their Lordships faced in reconciling the definition of 'personal data' in the DPA with the spirit of Directive 95/46/EC and in particular with Recital 26 of the Directive which states that 'the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. Indeed, Baroness Hale stated that '[while their Lordships would] all like the legal position to be that, if the risk of identification [of the children] can indeed be eliminated, the Agency is obliged to provide [the information requested]',[22] in line with the 'expectation in Recital 26', she had 'much more difficulty in spelling out [that conclusion] from the definition of "personal data" in section 1(1) of the Act'.[23] The foregoing analysis indicates that the attempt to protect privacy through regulation of processing of personal data is fraught with difficulties, due to the confusion surrounding the concept. The decision does not clarify how the 'identifiability' requirement should be interpreted and applied in future cases. Also, questions remain as to precisely what factors are to be taken into account in determining when data can be said to be 'fully anonymised' and as such, no longer personal data.

Relationship between 'personal' and 'private' data

Moreover, the absence of a concept of 'private' data in the Directive and DPA 1998 and the fact that privacy protection is to be achieved through the regulation of the conditions under which personal data may be processed, *prima facie* suggests that the terms 'personal' and 'private' are synonymous, or alternatively, that protection of personal data effectively protects privacy. Yet, there is a lack of research data the effectiveness of the model of privacy protection advocated in the Directive. This article seeks to remedy that deficiency by reporting the findings of interviews with privacy and data protection experts, and also the responses from a survey of bloggers.

Research method

To answer the questions posed, data was collected in two phases. First, semi-structured interviews[24] were conducted with forty privacy and data protection experts, namely: privacy commissioners, lawyers, corporate privacy officers, consultants, computer

scientists and academics from sociology, politics, market research, statistics and law.[25] The second phase of the data collection process consisted of an online survey of bloggers from around the world.[26] Out of the total number (1314) of responses received, 1258 were selected for data analysis; the remainder of responses were incomplete and were disregarded. However, the resulting population of participants does not qualify as a random sample and, accordingly the results from this survey cannot be generalised to the entire blogging population.[27] Rather, the findings are representative of certain niches of the English-speaking blogging world.

Research findings

(1) Views of data protection and privacy experts

All respondents were familiar with the concept of personal data as they had knowledge of the EU Directive 95/46/EC or it had been implemented into their national legislation, but indicated difficulties in drawing the lines between 'personal' and 'not personal' data. Some discussed the fact that technological developments are causing difficulties, e.g. advances in genetics are leading to greater pressure to collect health data and, while this is often stored and processed in the form of 'coded' data, there is a lack of clarity whether such data should be considered personal data. Another example cited was transaction data/behavioural data on the internet, e.g. clickstream data can lead to a profile being created which may, or may not, be considered personal data. When asked whether the concepts of personal and private data are synonymous, a range of responses were recorded. They have been classified under four broad headings:

(i) *Private concept not legally recognised. Informally it is synonymous with personal data*

> I think in a legal sense – in a data protection sense, yes (the terms private and personal are synonymous). However, privacy protection and data protection are different, but in a colloquial sense they are synonymous. (Belgium)

> In our law the word 'private' isn't even used, so it doesn't have a legal meaning. The general population take them to mean the same thing. (Canada)

The experts drew a distinction between personal data that is protected in law and private data that is not legally recognised, but which in the mind of the general public, is a synonymous term. When asked to elaborate on the concept of private data, they stated:

(ii) *Private data is a subset of personal data that the individual wants to keep absolutely secret*

> Private data is the part of the personal data that the respondent does not want to make public. (Spain)

(iii) *Private data is a subset of personal data that the individual wants to control access to or reveal in limited circumstances*

> It is something not revealed to others, or only revealed to a select group. It is a concept close to confidentiality but without the legal connotations, e.g. disclosure to a family member/bank/personnel office e.g. my salary would be considered private. (New Zealand)

> Personal data is data relating to an individual . . . . Private data is something you want to keep to yourself or something that people need to seek your permission to give out. (Australia)

These responses imply that individuals will face choices regarding disclosure of information and that the individual providing the data should decide the nature and extent of disclosure. These responses reflect the informational control conception of privacy espoused by Westin, who defined privacy as the

> claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[28]

Similarly, in the German census case[29] the notion of 'informational self-determination' was advocated. The German Constitutional Court ruled that

> This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest.[30]

However, while the experts identified private data as a subset of personal data that merits extra legal safeguards in order to protect privacy, they did not offer clearly delineated boundaries for this term, which could be of general application. Instead, the comments below illustrate that, in their experience, claims that information is 'private' arise on an *ex post facto* as opposed to *ab initio* basis.

(iv) *All personal data can be private, depending on contextual factors*

> They are not synonymous. Private, is an *ex post facto* term, used mainly to label those claims for non-disclosure that we've accepted on other contextual grounds. Whereas, the term personal, concerns information about which less contested claims are made, e.g. the personal fact that I'm bald and short-sighted is personal data but it is hardly a private fact. (UK)

> Personal data can become private. . . . Some pieces of data we don't want to go elsewhere are what we consider private – but it depends on the company, e.g. happy for A to know but not B to know. (UK)

> If data is generally personal, it may become private depending upon place, time and circumstances . . . in different circumstances people see the same data differently, therefore, it is very difficult to define this kind of data. For example, if we approach our bank manager for a loan then we will be willing to discuss our salary but, in other circumstances you won't tell someone your salary. (Finland)

The responses from the data protection and privacy experts embody the philosophical ideals of autonomy and dignity through 'informational self-determination'. The experts recognise that a data subject should have the right to a degree of control over information that identifies them or relates to them, since control over disclosure identifying information is necessary for the development of autonomous individuals. They further acknowledged that it is not possible to predict in advance what personal information will be claimed as private by a data subject, since such claims are usually made on an *ex post facto* basis, depending on contextual factors.

(2) Views of bloggers

In the survey, almost one-quarter (24.8%) of respondents said that they had posted personal information on their blog 'all the time'.[31] However, bloggers seem to reflect regularly on the content of posts when deciding whether or not to post personal information online. Most

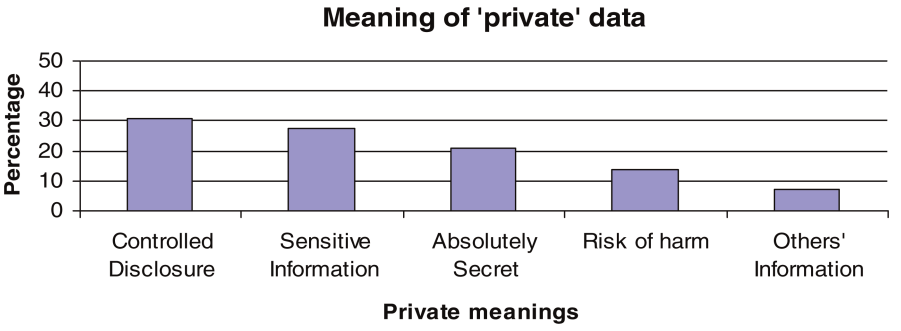

Figure 1. Graph illustrating meaning of 'private' data (source: Blog Survey 2006, $n = 101$).

respondents (65.6%) said they had considered some information 'too personal' or 'private' to write about on their blogs.[32] Respondents who stated that 'private' data did not mean the same as information which is 'too personal' (36.5%) to write about in their bogs were asked to explain what private information meant.

The largest percentage (30.7%) equated private with '*controlled disclosure*'. It is information which the individual wants to control access to, or disclose in limited circumstances. Below are some illustrative comments:

> Some information that I might want to discuss with only a select few .... Then I would make that entry a secure one, so that only those people belonging to that group could read and comment. It is not information that I consider public, but neither is it too personal to share.

> Private' information varies – there's stuff you'd share with friends, then only close friends, or nobody at all.

These responses mirror the responses of the experts and reflect the informational control conception of privacy, as they indicate that bloggers are aware that they constantly face choices about the nature and extent of information disclosures they make on their blog posts.

Private data was equated with either legally recognised or potential new categories of '*sensitive data*' by just over one-quarter (27.6%) of respondents, as illustrated by comments

> Private information is data about me as an individual such as biometrics, financial, political beliefs etc. Things which are too personal are to do with relationships with other people, etc.

> Private information, to me, describes data (financial information, phone number, etc.), whereas 'too personal' describes emotional information (how I felt about something my friend said last week).

These responses encapsulate the definition of privacy offered by Innes who stated that it is 'the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information and intimate actions'.[33] According to this view of privacy, not every disclosure of information about a person will amount to a loss of privacy; there will only be a loss when 'sensitive' or 'intimate' personal information is disclosed.[34] The responses indicate that bloggers are aware of such distinctions and actively limit disclosure of such information on their blogs.

It is information which the individual wants to keep '*absolutely secret*' was the meaning attributed to 'private' information by one fifth (20.8%) of respondents, as illustrated by comments:

> Private is information that I don't want to discuss with anyone.
>
> Information I would not trust other people with. It doesn't have to be 'personal' in the sense of intimate. It could be financial details, for instance.

A minority of bloggers (13.9%) equated 'private' data with the '*risk of harm*' arising from data uses:

> Private information, when it comes to an on-line environment, refers to any data which a third party having knowledge of could cause me actual harm, whether financial, or by restrictions of civil liberties. This therefore refers to my financial details, address and contact details (though to a lesser degree).
>
> Private information is information I don't want total strangers to have (e.g. home address), or that could be used to cause me a harm (monetary or otherwise, e.g. credit card and PIN numbers).

'*Information about others*' was the meaning attributed to private data by the lowest number of respondents (6.9%):

> This is information like the names of people I am writing about if they are not in the public arena or making them identifiable in some other way if I haven't asked.
>
> I don't write things that are too personal about my friends and family. I don't paraphrase them or post IM [Instant Messenger] conversations without running it by them first. I don't use other people's first names unless they have their own blog that they have given me permission to link to where they use their own first names.

These responses also indicate that bloggers are aware that the notion of privacy hinges on the concepts of control and consent regarding disclosure. Thus, each individual should decide for themselves the nature and extent of information which is disclosed. Also, there may be circumstances in which an individual does not have direct control over their personal information, but their privacy is nonetheless respected, e.g. a blogger does not post information about friends without express or implied consent. Indeed, the responses indicate that bloggers are aware that some information is shared in the context of a variety of relationships and that maintaining confidentiality and secrecy in respect of such information is a necessary requisite for healthy functioning relationships. These responses fall within the 'intimacy' conception of privacy espoused by Fried who, defined privacy as the 'control over knowledge about oneself'.[35] He based his definition of private information on intimate relationships by asserting that privacy should be valued because it is necessary to protect 'fundamental relations' of 'respect, love, friendship and trust'.[36]

Criticisms of current approach **Q2**

The complexity surrounding the concepts of privacy, private and personal data is evidenced by the responses from experts and bloggers. The responses reveal that there are no consistently agreed meanings attached to any of the terms, and indeed, these terms are often used interchangeably and in an overlapping fashion. One reason for this is that the data

protection principles are stated in broad, general terms, rather than in specific terms capable of precise legal delineation. However, Art. 22 of Directive 95/46/EC requires EU member states to provide a right to a judicial remedy for a breach of any of the rights guaranteed by the Directive. This means that UK Courts must necessarily confer some precise meaning on the general principles. The *Durant* decision illustrates the difficulties posed by this requirement. In that case the Court attempted to apply a purposive approach – asserting that because the purpose of the access right is to protect the privacy of the data subject, it is only information that is relevant to that purpose which can be subject to the access right. However, this approach is artificial and unhelpful, as it misconceives the role of personal data in determining the scope of privacy within data protection legislation. It also fails to recognise that data protection legislation serves other interests, e.g. data accuracy and data quality.

An alternative 'harm' based approach to privacy protection

The responses from the data protection and privacy experts embody the philosophical ideals of autonomy and dignity through 'informational self-determination'. The experts recognise that a data subject should have the right to a degree of control over information that identifies them or relates to them, since control over disclosure identifying information is necessary for the development of autonomous individuals. However, although control may in fact protect privacy in many circumstances, equating control with privacy is not always effective. For instance, individuals may be provided with control and subsequently decide to give up their privacy. Alternatively, once information is shared with another, e.g. in the course of a friendship or business transaction, an individual no longer has exclusive control over the disclosure of the information. Yet, the individual's privacy may (as a matter of good customer relations, or in the interests of sustaining a friendship), or may not, be protected in the absence of direct control over the information. Moreover, the responses by bloggers and experts acknowledge that it is not possible to predict in advance what personal information will be claimed as private by a data subject, since such claims are usually made on an *ex post facto* basis, depending on contextual factors. Accordingly, some of the experts were critical of the underlying approach of the Directive, claiming that the current model of privacy protection which is based on collection limitation principles is outdated. They assert that it regulates at the wrong level and fails to balance competing interests properly. The Directive regulates the collection and processing of data, as opposed to regulating specific harmful uses of the data:

> There is a realisation that information is gathered, collected. It [data collection] is ubiquitous and [it is] impossible to chase wrongful collection; therefore, the focus has shifted towards a harm-based approach. (USA)

Accordingly, they contend the focus of regulatory activity should shift. It should centre on harm related to the misuse of personal information.

> Regulation of collection is a losing battle – instead ensure it is not used malevolently – information will always need to be collected, so you need to focus work on how it is used. (Australia)

Both bloggers and privacy experts recognised that personal data can be used or misused. The interchangeable and overlapping uses of the terms personal and private data by bloggers indicate that the focus of data protection legislation has erroneously been on the

categorisation of data into personal or sensitive data, and the limitation of collection of such data, instead of the harm arising from data uses.

Conclusion

The foregoing analysis indicates that the decision in *Durant* v. *FSA* is at odds with the general principles of data protection. It attempts to limit the scope of personal data. While this approach is *prima facie* useful from privacy perspective, it fails to recognise that data protection legislation also serves other interests and that a broader interpretation of personal data is necessary to achieve these purposes. This failure undoubtedly reflects the notorious difficulties that have plagued attempts to give privacy a precise, analytically serviceable and universally accepted meaning. The failure to define 'private' data in data protection laws has a cost, in so far as it detracts from the capacity of those laws to offer prescriptive guidance. A further cost is that it perpetuates the vulnerability of the privacy concept to the criticisms that it is incapable of definition, has no independent, coherent meaning and should be subsumed by other concepts.

It is suggested that the time is ripe to review the provisions of the Directive as the focus of the current legislative model is erroneously on the categorisation of data into personal and sensitive data, and the application of different levels of privacy protection to the different categories of data. The responses of the experts and blogggers indicate that, in the information society, the notion of privacy has changed. In this era, privacy is the absence of harmful use and application of information about an individual. As the UK Information Commissioner stated, the Directive 'out of date, bureaucratic and excessively prescriptive. It is showing its age and is failing to meet new challenges to privacy, such as . . . the huge growth in personal information online.' This paper echoes the Commissioner's call for a review of the legislation. In particular the interpretation of the concept of personal data should be reviewed. It is suggested that it should receive a 'broad' interpretation and the question of when information is 'identifiable' should be answered using a risk of re-identification approach. Also, the concepts of consent and control should be revisited. Further research is needed on the concept of consent. It may be worthwhile developing a test for implied consent in order to achieve a balance between privacy interests and the legitimate interests of others. Also, future legislation could focus on regulation of specific harmful uses of personal data and the availability of appropriate remedies.

Notes

1. Information Commissioner's Office (ICO), 'UK Privacy Watchdog Spearheads Debate on the Future of European Privacy Law', ICO, Wilmslow, Cheshire, 2008. Available at http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_leads_debate_070708.pdf
2. *Durant* v. *FSA* [2003] EWCA Crim 1746.
3. *CSA* v. *SIC* [2008] 1 WLR 1550, [2008] UKHL 47.
4. The issue has occupied the minds of scholars and jurists alike for decades. It is a common feature of any privacy analysis to start with a disclaimer about the inherent difficulty or impossibility of defining exactly what privacy is or, of dissecting the concept into its various components. While the definitions espoused by Judge Cooley, Samuel D. Warren and Louis D. Brandeis, Alan Westin have a certain intuitive appeal, none have become universally accepted.
5. D. Korff, 'Comparative Study of National Laws', EC Study on the Implementation of Data Protection Directive, 2002, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf
6. Ibid.

7. S. Booth, R. Jenkins, D. Moxon, N. Semmens, C. Spencer, M. Taylor and D. Townend, 'What are "Personal Data"? A Study Conducted for the UK Information Commissioner', 2004, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/final_report_21_06_04.pdf
8. *Durant* v. *FSA* [2003] EWCA Crim 1746.
9. Identifiabililty was not an issue because the information in the manual files essentially comprised letters of complaint written by Mr Durant and material generated in response to his complaint.
10. *Durant* v. *FSA* [2003] EWCA Crim 1746, [27].
11. Ibid., [28]
12. Ibid.
13. Ibid.
14. Ibid.
15. See European Court of Justice decision in *Bodil Lindqvist* v. *Kammaraklagaren* (2003) C-101/01, para. 27, as referred to in para. 28 of the Durant judgment.
16. Ibid. **Q4**
17. Art. 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf)
18. ICO, 'Data Protection Technical Guidance – Determining What is Personal', v1.0, 21 August 20007, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf
19. *CSA* v. *SIC* [2008] 1 WLR 1550, [2008] UKHL 47.
20. The corresponding provisions of the Freedom of Information Act 2000 are in materially the same terms and the judgment is therefore of relevance throughout the UK.
21. A specialist health board in Scotland which collects statistical information from other health boards.
22. *CSA* v. *SIC* [2008] UKHL 47 [91]. **Q5**
23. Ibid., [92].
24. In the interviews semi-structured questions were used. The aim was to have a discussion with the respondent so that all the themes in the interview guide were covered. Some of the themes in the interview guide were too complex for a few of the participants. For instance, statistical methodologists were not comfortable when answering questions about the specific detail of the legislation in their country.
25. A respondent matrix was created using quota and snowball sampling. Snowballing is an effective technique for building up a reasonable sized sample, especially when used as part of a small-scale research project (M. Denscombe, *The Good Research Guide for Small Scale Social Research Projects* (Milton Keynes, UK: Open University Press, 1998).
26. The respondents were not randomly selected but were found through a variant of the snowball-sampling strategy. Announcements for the online survey were posted to mailing lists in three universities in the UK area as well as on a few high-traffic blogs. The viral nature of blogs meant that the links to the survey page quickly spread to many other blogs and YouTube.
27. It is the bloggers' subjective sense of privacy and liability that is revealed. This self-disclosure approach has three important implications: (1) There can be disparities between stated privacy attitudes and actions; (2) Participants' perceptions of their blogs might differ from those of outside observers and researchers; (3) accuracy is difficult to verify, e.g. no external validation was conducted.
28. A.F. Westin, *Privacy and Freedom* (New York: Atheneum Press, 1967), 7.
29. BVerfGe 65, 1. The text is available at http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm **Q6**
30. BVerfGE 65, 1 – Volkszählung, 1983.
31. Only 2% of respondents said they had 'never' posted anything highly personal on their blogs.
32. It is important to note is that a consensus of definition does not exist regarding the terms private or personal. Indeed many used the terms interchangeably.
33. J.C. Innes, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992), 140.
34. Ibid., 58.
35. C. Fried, 'Privacy', *Yale Law Journal* 77, no. 3 (1968): 483.
36. Ibid., 477.