Data sensitivity: proposals for resolving the conundrum

Mccullagh, K

Data Sensitivity: Proposals for Resolving the Conundrum

Karen McCullagh[1]

Abstract: The EU Directive 95/46/EC specifically demarcates categories of sensitive data meriting special protection. It is important to review the continuing relevance of existing categories of sensitive data in the light of changes in societal structures and advances in technology. This paper draws on interviews with privacy and data protection experts from a range of countries and disciplines and findings from the Information Commissioner's annual telephone survey of the British public in order to explore satisfaction with the current categories of sensitive data. It will be shown that the current classification of sensitive data appears somewhat outdated and thus ineffective for determining the conditions of data processing. Finally, possible reform proposals will be reviewed, including a purpose-based approach and context-based approach.

1. Origins of Protections for Sensitive Data

The concept of 'sensitive' data was first considered for introduction into international law by the expert group drafting the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).[2] Sweden and the German state of Hesse had already incorporated the concept into national and state law.[3] Ultimately the drafters of the Guidelines decided not to include extra safeguards for designated categories of sensitive data. The absence of safeguards seems to be partly due to a failure to achieve consensus on which categories of data deserve special protection, as the guidelines state:

> ...it is probably not possible to define a set of data which are universally regarded as being sensitive. (para 19 (a)).

Moreover this approach may also reflect the belief that personal data is not categorically deserving of protection, but instead that appropriate protection is dependent upon the context in which the data are used.

Although the Guidelines are not binding on OECD Member States, they have influenced the enactment of data protection legislation in both EU and non-EU member countries, such as Australia, New Zealand and Hong Kong. Recently, the twenty one Asia-Pacific Economic Cooperation (APEC) member economies[4] adopted the *APEC Privacy Framework*, which claims that its Framework is 'consistent with the core values' of the Guidelines.[5] However, since the guidelines were not legally binding on any of the member countries, they did not serve as the international data protection law that they were intended to be (Walczuch & Steeghs, 2001). Indeed, experts opined that the guidelines overemphasised the principle of unrestricted trans-border data flows at the expense of the privacy interest of the data subjects (Ellger, 1987).[6] Furthermore, Kirby[7] conducted a review of the Guidelines and suggested that they need to be updated to include new privacy principles appropriate for contemporary technology, such as internet based automatic profiling.

---

[1] PhD candidate, CCSR, University of Manchester, Email: <Karen.mccullagh@postgrad.manchester.ac.uk> This researcher is sponsored by the ESRC and Office of The Information Commissioner, UK. All views expressed in this article are those of the author and do not necessarily represent the views of, and should not be attributed to either of the Sponsors.

[2] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[3] The emergence of data protection laws, starting in Hessen (Hesse is English translation) 1970 and Sweden 1973, was closely linked to use of computer technology as a tool for collecting and distributing personal data. See Sieghart, P. (1976), *Privacy and Computers*, Latimer, London.

[4] There are 21 member economies. See: http://www.mapsofworld.com/apec-member-economies.htm

[5] Greenleaf claims that The Framework is in fact weaker in significant respects than the OECD Guidelines, to some extent in its principles but particularly in its implementation requirements. Greenleaf, G. (2005) "APEC's Privacy Framework: A new low standard," *Privacy Law & Policy Reporter* Vol. 11 No 5, 121- 125

[6] Ellger, R. (1987), "European data protection laws as non-tariff barriers to the transborder flow of information," in Mestmaecker, E.-J. (Ed.), *The Law and Economics of Transborder Telecommunications, A Symposium,* Nomos Verlagsgesellschaft, Baden-Baden, 121-43.

[7] Kirby, M. (1999) "Privacy protection, a new beginning: OECD principles 20 years on," *Privacy Law & Policy Reporter*, Vol. 6 No 3, 25-30

Thereafter the concept of sensitive data was introduced into international law through the Council of Europe Convention For The Protection of Individuals With Regard To Automatic Processing Of Personal Data (1981).[8] Although the Explanatory Report[9] advocates a context based approach to determining risk of harm from personal data processing, it recognises exceptional cases where the processing of certain categories of data may encroach on individual rights and privacy interests.[10] These 'sensitive' categories are listed in Article 6 as:

> Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Paragraph 44 of the Explanatory Report states that "revealing ... political opinions, religious or other beliefs" also covers activities resulting from such opinions or beliefs. Paragraph 45 indicates that "personal data concerning health" includes information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased. This category of data also covers those relating to abuse of alcohol or the taking of drugs.

The categories listed in Article 6 are not meant to be exhaustive. Rather, the Convention provides that a Contracting State should be free to include other categories of sensitive data. Data sensitivity depends on the legal and sociological context of the country concerned:

> Information on trade union membership for example may be considered to entail as such a privacy risk in one country, whereas in other countries it is considered sensitive only in so far as it is closely connected with political or religious views. (para 48)

The Council of Europe Convention, in contrast with the OECD guidelines, had to be incorporated into domestic law by the countries that acceded to it. However, not all the Member States passed data protection laws and in those which did, the laws were not all consistent with one another. For instance, the UK law did not cover any manual data , whereas the Hesse data protection law did. The UK had a detailed system of registration, whereas others did not.[11] Hence, the Convention did not succeed in bringing about the full harmonization of data protection laws.

Subsequently, the United Nations issued **Guidelines for the Regulation of Computerized Personal Data Files** (1990)[12] **,** which addressed the issue of sensitive data under a *Principle of non-discrimination.* The Guidelines defined such data as:

> …data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.[13]

This international treaty is broader than the Council of Europe convention (discussed above), as it includes the categories ethnic origin and colour. In addition, it includes membership of trade unions or other associations. However, it does not include criminal convictions or health data. Both the convention and the guidelines provided for States provide opportunities to regulate risks stemming from the processing of personal data by applying an internationally approved regulatory model. Indeed, they remained free to enact rules that better fulfilled their requirements, or even to abstain from any legislative action. Table 1 displays the categories of data listed as sensitive in the three international legislation discussed in the preceding section.

[8] European Treaty Series - No. 108, (28.I.1981), http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
[9] http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm
[10] Paragraph 43.
[11] Jay, R. (2004) "The Data Protection Act 1998 (DPA)" JISC Legal Information Service Briefing Paper
[12] Adopted by General Assembly resolution 45/95 of 14 December 1990
[13] http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm Principle 5

Table 1: Categories of sensitive data in International Legislation

OECD Guidelines (1980)	Council of Europe Convention (1981)	UN Guidelines (1990)
None	Racial origin	Racial or Ethnic origin
	Political opinions	Political opinions
	Religious or other beliefs	Religious/philosophical/other beliefs
	Sexual life data	Sex life
	Health data	Membership of a trade union
	Criminal convictions	Membership of an association
		Colour

As time passed, an increasing number of countries introduced data protection laws and tighter restrictions on trans-border data flows across national borders were implemented. Many countries with strong data protection interdicted the transfer of protected data to countries with less strong or no data protection measures. This severely impeded the business of some multinational companies. An example of this occurred in 1989, when French authorities halted the transfer of personnel records from Fiat's French office to the Italian base office because Italy had no data protection legislation at that time, while France had high levels of protection (Mei, 1993).[14]

1.1 Current EU definition of sensitive data

In order to remove obstacles to the free movement of data without diminishing the protection of personal data, the European Commission decided to harmonize data protection and proposed Directive 95/46/EC (the Directive).[15] The Directive includes a provision that sensitive data must be more stringently protected.[16] Such data is defined in Article 8 (1) as:

> Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … data concerning health or sex life.

Article 8(5) also makes special provision for criminal records and the like:

> Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable safeguards…

Thus, the principle of sensitivity holds that the processing of eight types of data should be subject to stricter controls than other types of personal data. The Directive differs from the Council of Europe's approach in two main respects: 1) it includes the trade union membership as a specific category of sensitive data; 2) the list is considered exhaustive, whereas the Council of Europe list is merely indicative. The Directive differs from the UN Guidelines as it lacks a category of data on colour or membership of association, but includes a category of

[14] Mei, P. (1993), `"The EC proposed data protection law," *Law and Policy in International Business*, Vol. 25, 305-34.

[15] http://europa.eu.int/comm/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf http://europa.eu.int/comm/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf

[16] In principle, such data cannot be processed. Derogation is permitted under very specific circumstances. These circumstances include the data subject's explicit consent, processing mandated by employment law, where it may be impossible for the data subject to consent (e.g. blood test to the victim of a road accident), processing of data has been publicly announced by the data subject or processing of data about members by trade unions, political parties or churches. Member states may provide for additional exceptions for reasons of substantial public interest.

criminal convictions. A more radical difference exists between the Directive and the OECD guidelines, in which drafters adopt a contextual approach and do not specifically enumerate special categories of sensitive data.

It is important to review the continuing relevance of existing categories of sensitive data in the Directive in the light of changes in societal structures and advances in technology. In the pre-computer era, data processing was not automatic and large-scale, uncontrolled surveillance was costly, thus providing natural barriers for privacy protection. These natural barriers disappeared gradually in the mid 1960s because computerized technology for processing an increasing amount of information needed to develop social welfare-states was available at faster speeds and lower costs.[17] Also, business organizations owning large amounts of records started to use computers. By the 21st-century, businesses are such that customers expect them to operate at all times. It is not only the e-commerce world that experiences this situation. All types of organizations - including health care, financial, manufacturing, and services operate around the clock, or at least their computer systems do. Even when no humans are around, computers are available to take and place orders, send orders to the warehouse, and manage financial transactions, all involving the processing of potentially sensitive personal information.

Several issues arise: firstly, are the current categories still considered sensitive? Secondly, have new categories of sensitive data emerged? If new categories have emerged, can the current legislation incorporate them? Should the list be extended or should an alternative approach be adopted? These issues were explored through semi-structured interviews with experts and findings from the Information Commissioner's annual telephone survey of the British public.

2. Current categories of sensitive data

2.1 Responses from expert interviewees

Interviews were conducted with thirty seven privacy and data protection experts from a range of disciplines, including privacy commissioners, lawyers, industry experts, statistical methodologists, computer scientists, and academics from a variety of disciplines including sociology, market research and law.[18] 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. Accordingly, the researcher was creative and aware of the need to see the issue from the interviewee's position and asked the questions in an appropriate but not leading way. The advantage of this approach is that it allowed a cognitive process to emerge, so that the information obtained from respondents provided not just answers, but reasons for the answers.

Some respondents were happy with the existing definition and the types of data covered. For example, one respondent stated:

> In the UK existing categories of sensitive data have merit in that they are associated with a right to human dignity/freedom of political activity. The difficulty with the current provisions is the overriding public interest tests, in the EU Directive there is a categorical prohibition on the processing of certain data – but it is subject to higher public interest tests…Existing categories of sensitive data are sensible. (UK)

Likewise,

> I'm broadly happy with existing definitions in Ireland. The approach taken in the Directive is correct. Sensitive data is an arbitrary list. (Ireland)

Others did not agree with all classifications,

> We had to introduce the concept of sensitive data in Iceland but we don't agree with all the categories e.g. according to the Directive data on trade unions is considered sensitive, but in Iceland such information is not as everyone knows where you work and what unions you belong to and they don't care about these things… (Iceland)

[17] Mayer–Schönberger 1997, 222, For a discussion of the connection between large databases and social welfare state. Mayer-Schönberger, V. (1997) Generational Development of Data Protection in Europe. *In* Agre, P E. & Rotenberg, M. (eds.) 1997. *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts, MIT Press.

[18] 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 (Denscombe 1998).

Also, some Interviewees suggested new categories of sensitive data. Below are some illustrations:

> Some regard or suggest financial data to be sensitive – in this regard the categorisation of it as non-sensitive is clearly arbitrary – it may be worthwhile amending the legislation to make it sensitive. (Ireland)

Interviewees indicated that technological developments are generating potential new categories of sensitive data, for example

> They could be expanded e.g. to include financial data. They could be ramified. E.g. for health data a biometric template[19] should probably be considered personal data but probably isn't sensitive data. Whereas, genetic information could be regarded as sensitive because of the potential for prejudice and unfairness of inappropriate disclosure. (UK)

The concept of data protection through legislation is essentially an issue of formal public policy recognition and protection being accorded to values and ideologies that are held to be important by individuals and that are institutionalized in any individual culture (Ajami,1990).Thus, it is important to ascertain if the legal definitions accord with the views of the public, who often play the role of a data subject, as government legislative initiatives are intended to give effect to the legal requirements of a society, and will only be successful if they are valued and supported by the public.

2.2 Findings from ICO Annual Track telephone survey of British public

The views of UK citizens regarding the concept of sensitive data were sought through the ICO Annual Track (Individual survey 2006).[20] The survey was designed to examine public perceptions of sensitive data. Firstly, it was used to test sensitivity ratings of seven categories of data which are currently recognised in the Directive as sensitive. Also, it was used to test perceptions of sensitivity towards eight not legally recognised categories of sensitive data which emerged in interviews with data protection and privacy experts. The 15 categories of sensitive data tested are displayed in Table 2.

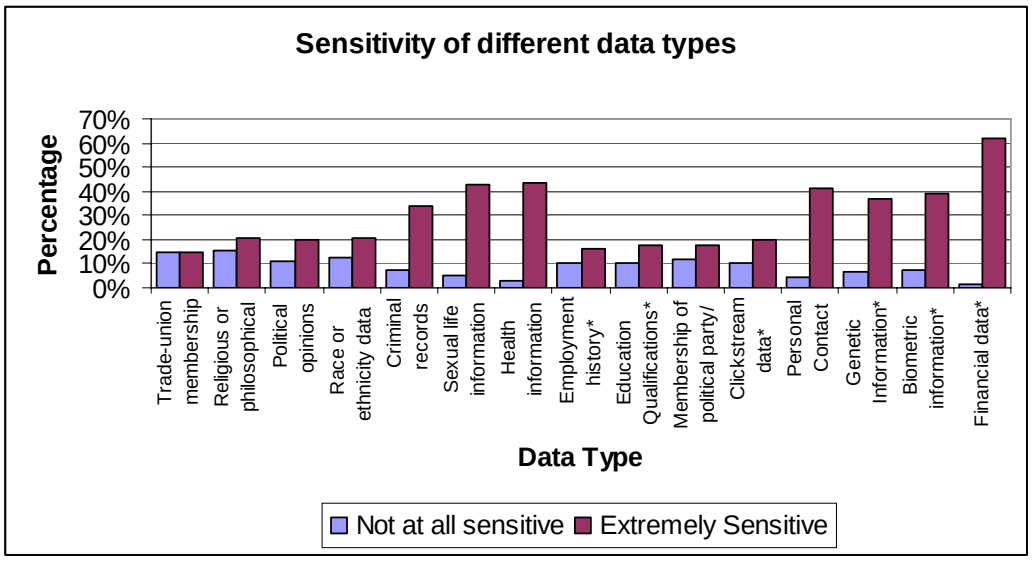
Table 2: *Classification of sensitive data*

Art 8 Legally recognised categories	Not legally recognised categories
Trade-union membership	*Employment history*
Religious or philosophical beliefs	*Education Qualifications*
Political opinions	*Membership of political party / organisation*
Data concerning race or ethnic origin	*Clickstream data (e.g. record of web pages visited)*
Criminal records	*Personal Contact Details*
Sexual life information	*Genetic Information*
Health information	*Biometric information (e.g. iris scans, facial scans and finger prints)*
	Financial data

[19] Biometrics comes from the Greek words *bios* (life) and *metrikos* (measure). The term refers to any specific and uniquely identifiable physical human characteristic, *e.g.*, of the retina, iris, acoustic spectrum of the voice (*i.e.*, voiceprint), fingerprint(s), handwriting, pattern of finger lengths, *etc.*, that may be used to validate the identity of an individual.

[20] The survey was conducted by telephone. All the interviews were conducted in house by SMSR's telephone interviewing team. The total sample was 1,066 interviews.[20] Quotas were set on age, sex, region and social grade to ensure a nationally representative sample was achieved.

Figure 1: *Sensitivity of different data types*



(Source: ICO Annual Track Survey 2006) (n=1066)

Fig. 1 shows how respondents rated different types of data on a scale of 1 to 10 with 1 being not at all sensitive and 10 extremely sensitive. The results indicate that of the legally-recognised types of sensitive data, health and sex life information were considered extremely sensitive by the highest percentage of respondents. However, some of the other categories were considered to be more sensitive than the legally-recognised types of sensitive data. For instance, financial data was considered extremely sensitive by most respondents (62.1%), while religious opinions were considered to be not at all sensitive by 15.3% of respondents. Likewise, more than one third of respondents rated biometric, genetic and contact details as extremely sensitive, whereas only one fifth of respondents rated data concerning race or ethnic origin, political opinions or data concerning religious or philosophical beliefs as extremely sensitive.

The 10 scale data rating was recoded into five categories (see Table 3). The data was analysed and is displayed in tables according to whether it is classified as legally recognised or not legally recognised as a category of sensitive data.

Table 3: Recoding of data sensitivity scale from 10 scale into 5 categories

Original value	Recode value	Category Label
1, 2	1	Not at all Sensitive
3, 4	2	A little Sensitive
5, 6	3	Sensitive
7, 8	4	Very Sensitive
9, 10	5	Extremely Sensitive

Table 4: *Sensitivity of legally recognised data types – ICO Survey*

	Trade-union membership	Religious or philosophical beliefs	Political opinions	Data concerning race or ethnic origin	Criminal records	Sexual life information	Health information
Don't Know	1.4%	.9%	.9%	1.3%	1.1%	1.6%	.9%
Not at All Sensitive	21.6%	21.4%	15.9%	19.5%	11.2%	6.8%	3.8%
A little Sensitive	13.9%	12.1%	13.1%	11.2%	7.2%	6.7%	5.1%
Sensitive	30.6%	28.2%	28.1%	1.3%	22.9%	18.0%	18.2%
Very Sensitive	15.1%	13.3%	17.4%	16.6%	17.5%	17.1%	20.6%
Extremely Sensitive	17.4%	24.0%	24.5%	24.6%	40.1%	49.8%	51.3%
	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

(Source: ICO Annual Track Survey 2006) (n=1066)

Table 4 displays the legally recognised categories of sensitive data and indicates that Health data was considered extremely sensitive by over half of the respondents (51.3%), and almost half considered sexual life information to be extremely sensitive, whereas fewer respondents considered religious or philosophical beliefs to be extremely sensitive (24%) and only 17.4% considered trade union membership data to be extremely sensitive. Thus, some of the legally recognised categories of sensitive data are considered less sensitive than others.

Table 5: *Sensitivity of not legally recognised data types- ICO Survey*

	Employment history	Education Qualifications	Membership of political party / organisation	Clickstream data (e.g. record of web pages visited)	Personal Contact Details	Genetic Information	Biometric information (e.g. iris scans, facial scans and finger prints)	Financial data
Don't Know	1.1%	1.4%	1.5%	2.5%	.4%	1.6%	2.2%	.6%
Not at All Sensitive	15.9%	15.9%	17.4%	15.9%	7.0%	8.7%	10.4%	1.9%
A little Sensitive	12.1%	11.7%	13.4%	11.4%	7.1%	6.3%	6.8%	2.5%
Sensitive	30.2%	29.5%	30.1%	27.5%	17.8%	20.8%	17.5%	7.1%
Very Sensitive	19.3%	19.5%	15.5%	18.2%	21.4%	19.2%	17.6%	17.4%
Extremely Sensitive	21.3%	22.0%	22.0%	24.4%	46.2%	43.3%	45.4%	70.5%
	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

(Source: ICO Annual Track Survey 2006) (n=1066)

Table 5 displays categories of sensitive data that are not legally recognised. The table indicates that financial data was considered extremely sensitive by over 70% of respondents, and just under half (46.4%) considered their personal contact details extremely sensitive, whereas only 21.3% of respondents considered employment history data to be extremely sensitive. The finding from the survey indicates that one fifth of telephone respondents considered trade union membership, religious/philosophical beliefs or data concerning racial/ethnic origin to be not at all sensitive.

However, further research is needed before imposing cut-off sensitivity points as 'sensitivity' is a value which has both an objective and subjective component. Buchholz comments,

> Values are different between people and reflect individual desires and beliefs. Values are properties that human beings associate with or assign to certain forms of human behavior, institutions, or material goods and services. (1992, p. 118)

From a subjective viewpoint, the sensitivity of a particular value is derived through individuals making personal judgements. In contrast from an objective perspective, the sensitivity of a particular value is derived outside the personal experiences of those individuals faced with choices. In this situation values are part and parcel of the behaviour or object in question. A complex interaction between these two perspectives leads to the creation of commonly held societal values that are believed to produce desirable outcomes for society as a whole (Buchholz, 1992; Daleiden, 1990). The conflict between the objective and subjective viewpoints is resolved through the essence of public policy formulation process, i.e. negotiation and compromise (Rule, 1974; Sieghart, 1984). Thus, further research is needed to test, for example, whether the respondents who indicated that race or ethnicity data was not at all sensitive were drawn from the majority white UK population, or whether similar views were expressed by the minority ethnic population.[21] Also, further research is needed to explain the reduced the sensitivity of such information, for instance, whether the Race Relations Act has been successful in protecting the rights and interests of ethnic minorities to the extent that such information is considered not at all sensitive by the UK population. Likewise, have changes in employment law for example equal opportunities[22] and minimum wage legislation reduced the sensitivity of trade union membership information?

The findings suggest that the current list is in need of reform, as *prima facie* it does not reflect the sensitivity perceptions of data subjects. Moreover, the findings suggest that new categories of sensitive data are emerging due to changes in society and technological developments. For instance, amidst post-September 2001 security concerns the UK government proposed the introduction of identity cards which rely on biometrics.[23] Such technology did not exist during the World-War II era when the UK previously utilised identity cards, and indeed they were removed from circulation in 1952, amid widespread public resentment.[24] This raises the issue of whether the current list of sensitive data could or should be amended? Is it possible to formulate an objective category of sensitive information despite claims that sensitivity is *relative* to the individual; and a function of the *context* in which the information is used rather than the type of information itself?

3. Criticisms of current approach

Korrf (2002)[25] conducted a comparative textual analysis of legislation. He found that the French, Austrian, British, Czech, Estonian, Finnish, Greek, Hungarian, Italian, Spanish, and Swiss laws state that the list their legislation contains is exhaustive, while, some countries (for instance, Denmark and Iceland) consider their lists as merely indicative. However, all laws provide ways and means to reopen the apparently closed list. For instance, the Estonian act states that the list can be modified by law, so *prima facie* the list of sensitive data categories could be amended.

However, creating new categories raises difficulties, for instance, Luxembourg, and the Netherlands define genetic data as data on *health*, whilst Portugal defines it as data on *health and sex life*, whereas in Sweden the processing of such data not formally regarded as falling within the specific category to which the rules on "*sensitive data*" apply. Hungary and Poland have added to Art 8 (1) "details of addictions". Many addictions would clearly fall within the health related category set out in the Directive already: for example drug addiction and alcoholism. Others, such as gambling or computer games, might not. It remains to be seen how regulators will interpret this additional restriction.[26] Thus, any attempts to modify or extend the current list would require transnational agreement otherwise a lack of harmonization will occur, and defeat the objective of the Directive.

---

[21] According to the 2001 12.5% of the population census across England and Wales are ethnic minorities. http://www.cre.gov.uk/diversity/ethnicity/index.html

[22] Employment Rights Act 1996, Sex Discrimination Act 1975, Equal Pay Act 1975, National Minimum Wage Act 1998

[23] Identity Cards Act 2006

[24] *Willcock v Muckle*, [1951] 2 The Times LR 373 The judge in the case said that the cards were an "annoyance" and "tended to turn law-abiding subjects into law breakers".

[25] Korrf, D. (2002) EC Study On Implementation Of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49)

[26] Linklaters (2004) Hot Topic: History repeats itself: the implementation of EU data protection legislation in the accession countries. http://www.linklaters.com/pdfs/briefings/040517_DP.pdf

Moreover, a definition-based approach has been criticised by some, as it would require a casuistic form of regulation, which is more complex and lengthy. Indeed, Bing[27] attempted to categorise all personal data according to their sensitivity. However, this approach was quickly abandoned, because it failed to delineate clearly the boundaries of the various spheres, why these exist and what might constitute a breach of the, for instance:

> Definitions of sensitive data are very subjective e.g. where you live is sensitive if you have an estranged violent husband. (UK)

Likewise, another respondent opined:

> I don't like the idea of sensitive data. All data is potentially sensitive, depending upon the context. (UK)

Simitis (1973)[28] asserts that detailed personal profiles could be created through the aggregation of ostensibly innocuous information, which could nevertheless have a detrimental impact upon a person's privacy. Thus, interviewees raised the importance of extraneous information, rather than simply relying on a definitional approach to sensitive data. The responses of several interviewees are exemplified by the following:

> I've never made much use of the concept, e.g. your postcode and newspaper preference both appear to be innocuous information. However, if you work for Experian (a credit score, credit report and credit reference agency), you can draw inferences about a person simply based on those two prices of information – that settles the point. How can you define what is sensitive? E.g. if you can work out my political views from my newspaper preference, then arguably my postcode and newspaper preference should be considered sensitive information. (UK)

Accordingly, some interviewees criticised the arbitrary nature of the exhaustive list base on definitions. At this juncture, it is appropriate to review alternative approaches.

4. Reform proposals: resolving the sensitivity conundrum

4.1 Context-based approach:

Simitis contends that personal data becomes sensitive according to its context. This mirrors the approach formerly adopted by countries such as Austria and Germany, which, prior to the introduction of the data protection directive had consistently rejected all abstract categorisations of personal data and instead focussed on a context-orientated consideration of the data. He asserts that

> Sensitivity is no more perceived as an *a priori* given attribute. On the contrary, any personal datum can, depending on the purpose or the circumstances of the processing be sensitive (Simitis,1999).

This approach reflects the opinions of some of the interviewees, for instance,

> Another example is related to the employment code we have drafted. Health is regarded as sensitive data. All employers keep records of sickness leave, but the issue is: does self-certified sick notes require the same level of protection as a medical note from a GP? Arguably a self-certified note is less sensitive, particularly given that the individual may have told colleagues the reason for their absence…yet no distinction is drawn in the law – but we would advise employers that they should take a common sense approach. (UK)

> The idea that all health information is sensitive is too restrictive in some instances e.g. it can cause difficulties between two contracting parties such as an insurance company and an individual. We need safeguards to protect sensitive uses of sensitive data. (Spain)

[27] Bing, J. (1972) "Classification of Personal Information with respect to the Sensitivity Aspect" Proceedings of the First International Oslo Symposium on Data Banks and Society, 98-141

[28] Simitis, S. (1973) cited in Bygrave, L. (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer, 132

Simitis reasoned that it is vital to consider contextual information when determining the sensitivity of data. Contextual information includes: the interests of the data controller as well as the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the individual and others. An evaluation of the sensitivity requires hence more than a definitional approach to sensitive data. Furthermore, Simitis advocates that sensitivity lists should be purely exemplary, and

> Only where the legislators can fully concentrate on a specific context, are they also able to reach a degree of precision that appropriately responds to the particularities of the processing circumstances. (Simitis, 1999)

This approach is more comprehensive than a definition-based approach, and more likely to reflect the concerns of data subjects. However it would be costly and difficult to implement, as Simitis recognises that it would need to be linked with sectoral regulation.

4.2 Purpose-based approach

In contrast, The Council of Europe (2005) proposed a purpose-based approach which would consider the purpose underlying the processing of personal data, that is, whether the processing is intended to reveal sensitive data.

> This approach would make it possible to consider the actual processing of data as sensitive rather that the data itself, even if no sensitive data were involved. For example, a search of trips to Rome conducted by a web surfer using Google or his or her purchases of religious books, reading of a papal encyclical, etc, may be treated as revealing a religious opinion. (Poullet *et al* 2004)

Searching for information on a trip to Rome would not in itself constitute processing of sensitive religious information, but when it is combined with searches for Vatican city visiting hours the purpose of the information processing may change. Of course, searches for such information may be purely coincidental, for instance if a person has heard that a restaurant within the Vatican grounds is worth a visit and checks the opening times etc.

The purpose-based approach mirrors the approach advocated by the OECD guidelines, namely that it is not possible to classify data as sensitive on a definitional basis. Instead, the actual processing of data, rather that the data itself could be considered sensitive. Moreover, Wacks[29] asserts that what changes from context to context is not the degree of sensitivity of information, but the extent to which one is prepared or required to allow it to be disclosed or used. Should the context change, it is not the nature of the information that changes, but an individual's *attitude* towards its use. An individual is likely to have considerably different views about the purposes for which sensitive data is used, for instance, an expert interviewee responded

> I think it will be extremely important to regulate who can access what information and for what reason e.g. whilst it may be acceptable to allow police to deduce racial information through DNA profiling it would not be appropriate to allow a security guard to have access to this type of information when simply determining if an individual should have permission to enter a building (UK)

Wong[30] contends that such an approach would reduce the number of trivial cases being brought before the courts, and also reduce the administrative burden placed upon data protection authorities. Additionally, it would shift the focus away from all data processors on to only those who intentionally reveal data of a sensitive nature. In essence, this is a teleological approach which seeks to prevent information being used in an unfair, harmful or discriminatory manner, and thus meets fulfils the original aim of the directive. However, Wong recognises that this approach leave an unanswered question, namely, *who* should decide what purpose is sensitive? Another unresolved difficulty is *how* to decide whether the purpose for which the data is processed is 'sensitive' if a definition-based approach is not used? No clear guidance is offered for data processors. Another undesirable consequence of this approach is that it pushes the decision regarding compliance away from rule makers onto already overburdened judges.

[29] Wacks, R. (1989) *Personal Information: Privacy and the Law*, Oxford: Clarendon Press, 23, 181
[30] Wong, R. (2007) "Data Protection Online: Alternative Approaches to Sensitive Data*?" Journal of International Commercial Law and Technology*, Vol. 2, No 1

4.3 A 'reasonable' approach to resolving the sensitivity conundrum:

It is suggested that a more radical approach should be adopted; one which recognises that the concept of sensitivity is an outdated concept. An expert interviewee opined that

> The concept of sensitive is a failed attempt to capture something, which isn't a natural kind. By saying something is sensitive you are attempting to treat something to do with claim for making different reasons in a single manner. Whereas, life is not reducible to a single algorithm – so you should be wary of this approach. (UK)

Instead of defining categories of sensitive data that deserve stricter protection, legislators should focus on the reasonableness of any request to process personal information. For instance, the province of Alberta, Canada has enacted privacy legislation[31] which does not distinguish between personal and sensitive information. Rather, it seeks to regulate the processing the collection, use and disclosure of personal information by private sector organizations

> in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are *'reasonable'*. (Emphasis added)[32]

The reasonable person test is an objective legal test. Thus an organization needs to be able to demonstrate that it considered the circumstances around handling personal information and made a decision on what is reasonable in the circumstances. The advantage of this approach is that it adopts a holistic approach to the contextual and purposive aspects of data protection. For instance, whilst it might be reasonable for a haulage company employer to insist that driver employees will be subjected to random alcohol for the purpose of ensuring work safety, it would not be reasonable for such an employer to require an employee to disclose any and all past alcohol problems. Mandatory disclosure would be unreasonable as it is too broad and intrusive and could have harmful discriminatory consequences for the employee.

5. Conclusion

It is suggested that the time is ripe to review the provisions of the Data Protection Directive. The current definitions reflect post World War II concerns regarding discrimination and protection of human dignity. In the 21st century , new concerns have risen ; for example, developments in the fields IT and biometrics are raising new potential categories of sensitive data. Indeed, findings from interviews and the survey indicate that whilst not all of the legally recognised categories of data continue to be perceived as sensitive, some which are not legally recognised categories of data are emerging which are considered extremely sensitive.

However, a decision to simply include new categories, or delete existing categories should not be taken lightly. Any attempt to grade data according to their sensitivity would be fraught with difficulties, as it would require a casuistic form of regulation, which is more complex and lengthy. Indeed, Bing[33] attempted to categorise all personal data according to their sensitivity. However, this approach was quickly abandoned, because it failed to delineate clearly the boundaries of the various spheres, why these exist and what might constitute a breach of them. For instance, detailed personal profiles could be created through the aggregation of ostensibly innocuous information, which could nevertheless have a detrimental impact upon a person's privacy. As Simitis[34] has shown , sensitivity of data varies from context to context. This contextual approach is more comprehensive than the purpose-based approach, as not only does it consider the purpose for which the data is collected, but also the conditions of processing and the possible consequences for the data subject. Moreover, Wacks[35] asserts that what changes from context to context is not the degree of sensitivity of information, but the extent to which one is

---

[31] The Personal Information Protection Act, (PIPA) does not apply to federally-regulated organizations such as banks, airlines, telecommunications companies and railways. Those organizations are governed by federal privacy legislation.

[32] The Personal Information Protection Act (PIPA) is in force as of January 2004 <http://www.oipc.ab.ca/pipa/>

[33] Bing, J. (1972) "Classification of Personal Information with respect to the Sensitivity Aspect" Proceedings of the First International Oslo Symposium on Data Banks and Society, 98-141

[34] Simitis, S. (1973) cited in Bygrave, L. (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer, 132

[35] Wacks, R. (1989) Personal *Information: Privacy and the Law*, Oxford: Clarendon Press, 23, 181

prepared or required to allow it to be disclosed or used. Thus, whilst categorisation of sensitive data serves a useful purpose of reminding data processors that unfair discrimination is prohibited, it should be understood as an indicative flexible, reference list. Finally, instead of trying to resolve the sensitivity conundrum, it would be prudent to consider the approach taken by other legislatures who advocate a 'reasonable' approach to data protection.

Bibliography

1. Ajami, R. (1990), "Transborder data flow: global issues of concern, values, and options", in Lundstedt, S.V. (Ed.), *Telecommunications, Values, and the Public Interest*, Ablex Publishing Corporation, Norwood, NJ
2. Bing, J. (1972) "Classification of Personal Information with respect to the Sensitivity Aspect" Proceedings of the First International Oslo Symposium on Data Banks and Society
3. Buchholz, R.A. (1992), *Business Environment and Public Policy: Implications for Management and Strategy*, Prentice-Hall, Englewood Cliffs, NJ.
4. Bygrave, L.A. (2002) *Data protection law: approaching its rationale, logic and limits*, The Hague: Kluwer Law International.
5. Daleiden, J.L. (1990), "Social considerations in the development of telecommunications policies", in Lundstedt, S.B. (Ed.), *Telecommunications, Values, and the Public Interest*, Ablex Publishing Corporation, Norwood, NJ.
6. Denscombe, M. (1998) The Good Research Guide. Open University Press.
7. Ellger, R. (1987), "European data protection laws as non-tariff barriers to the transborder flow of information", in Mestmaecker, E.-J. (Ed.), *The Law and Economics of Transborder Telecommunications*, A Symposium, Nomos Verlagsgesellschaft, Baden-Baden, 121-43.
8. Greenleaf, G. (2005) "APEC's Privacy Framework: A new low standard," *Privacy Law & Policy Reporter*, Vol. 11 No 5, 121- 125
9. Jay, R. (2004) "The Data Protection Act 1998 (DPA)" JISC Legal Information Service Briefing Paper
10. Kirby, M. (1999) "Privacy protection, a new beginning: OECD principles 20 years on," *Privacy Law & Policy Reporter*, Vol. 6 No 3, 25-30
11. Korrf, D. (2002) EC Study On Implementation Of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49)
12. Linklaters (2004) Hot Topic: History repeats itself: the implementation of EU data protection legislation in the accession countries. <http://www.linklaters.com/pdfs/briefings/040517_DP.pdf> Last Accessed May 2007
13. Mayer-Schönberger, V. (1997) "Generational Development of Data Protection in Europe," in Agre, P E. & Rotenberg, M. (eds.) (1997) *Technology and Privacy: The New Landscape*, Cambridge, Massachusetts, MIT Press.
14. Mei, P. (1993), "The EC proposed data protection law," *Law and Policy in International Business*, Vol. 25, 305-34.
15. Poullet Y., & Dinant, J-M., (2004) Report On The Application Of Data Protection Principles To The Worldwide Telecommunication Networks: Information Self-Determination In The Internet Era, Thoughts On Convention No. 108 For The Purposes Of The Future Work Of The Consultative Committee (T-PD)
16. <http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/T-PD%282004%29rapport_Poullet.pdf> Last accessed February 2007
17. Rule, J.B. (1974), *Private Lives and Public Surveillance: Social Control in the Computer Age*, Schocken Books, New York, NY.
18. Sieghart, P. (1984), "Information privacy and the data protection bill", in Bourn, C. and Benyon, J. (eds), *Data Protection: Perspectives on Information Privacy*, University of Leicester, Leicester.
19. Sieghart, P. (1976), *Privacy and Computers*, Latimer, London.
20. Simitis, S. (1999) Revisiting sensitive data,
21. <http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/Documents/Reports/W-Report%20Simitis.asp#TopOfPage> Last accessed February 2007
22. Wacks, R. (1989) *Personal Information: Privacy and the Law*, Oxford: Clarendon Press
23. Walczuch, R. M. & Steeghs, L. (2001) "Implications of the new EU Directive on data protection for multinational corporations," *Information Technology & People*,
24. Vol. 14 No. 2, 2001, pp. 142-162.
25. Wong, R. (2007) "Data Protection Online: Alternative Approaches to Sensitive Data?" Journal *of International Commercial Law and Technology*, Vol. 2, No 1