BILETA
British & Irish Law, Education and Technology Association
21st BILETA Conference:
Globalisation and Harmonisation in Technology Law
April 2006, Malta.

A study of data protection: harmonisation or confusion?[1]

Karen Mc Cullagh
University of Manchester

Abstract

The development of a frontier-free Internal Market and of the so-called 'information society' have resulted in an increase in the flows of personal data between Member States of the EU. To remove potential obstacles to such flows and to ensure a high level of protection within the EU, data protection legislation has been introduced.[2] *Further, it is claimed that through 'safe harbour' provisions and 'third country status' these measures are having an impact in other non EU countries.*

An attempt to assess whether 10 years after its inception harmonization of data protection concepts has in fact been achieved necessitated an exploration of the views of those operationalising it in the course of their employment as data controllers and those interpreting it on behalf of the general public. Semi-structured interviews were used to explore their understanding of and satisfaction with current definitions personal and sensitive data.

A stated aim of the directive is harmonisation of data protection within the EU. So, in theory there should be a common understanding and application of concepts such as personal and sensitive data. However, preliminary findings suggest that although the global village is now governed by similar data protection rules - harmonisation remains much more apparent than real.

Keywords: data protection, personal, sensitive, harmonisation.

---

[1] Karen Mc Cullagh, CCSR, University of Manchester. Research funded by ESRC and supported by Office of Information Commissioner, UK. <Karen.mccullagh@postgrad.manchester.ac.uk>

[2] Since 2004 the EU Data Protection Directive of 1995 is enforceable across the 25 EU Member States.

1. Legislative background

The European Commission aimed to harmonize data protection through the Directive on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data (95/46/EC) (*the directive*).[3] The directive applies to personal data processed wholly or partly by automatic means, and to manual data held in filing systems structured by reference to individuals.[4] It does not apply to areas within Titles V and VI of the Treaty of the European Union, namely public safety, defence, state security (including the economic well-being of the state when it relates to security matters), and the activities of a state in relation to criminal law. It also specifically excludes domestic or household activities. Certain 'sensitive' categories of information which reveal information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life and data concerning offences and criminal conditions may only be processed under certain strict conditions (Article 8).

The general purpose of the directive is to establish a set of rules capable of broad application and impact. Hence, in theory harmonisation should have occurred and the personal data of all citizens should have equivalent protection across the Union. However, whilst a directive prescribes an end result, the form and methods of the application is a matter for each Member State to decide for itself. Also, it is posited that the directive has additional political and legal influence in countries outside the EU because it prohibits the transfer of personal data to these countries unless they provide 'adequate' levels of protection (Arts 25-26). The directive also sets out the conditions under which personal data that is being processed may be transferred to countries which are not EU member states, but which are in the European Economic Area,[5] generally prohibiting the transfer unless the third country has adequate data protection measures in place.[6]

---

[3] 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

[4] The UK successfully petitioned for derogation in respect of manual filing systems. They must be made to comply with the directive by 24th October 2007.

[5] 3 non- EU members of the EEA (Iceland, Liechtenstein and Norway) ratified the directive. However, the Isle of Man and Channel Islands are outside the EU.

[6] E.g. USA 'Safe harbour' Principles

Consequently, this paper seeks to draw on previous studies and interviews with data protection and privacy experts to explore whether, 10 years after its inception, harmonization has in fact been achieved or whether it remains an idealistic myth.

2. Impact on Non EU Countries

The directive and subsequent legislation on data protection[7] were incorporated into the Agreement on the European Economic Area of 1992,[8] so that states which are not members of the EU but which are party to the Agreement, e.g. Norway, Iceland and Liechtenstein, are legally bound to ensure that their national laws conform with the provisions of the directive. Additionally, the Council and the European Parliament have given the Commission the power to determine, on the basis of Article 25(6) of directive, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.[9] The effect of such a decision is that personal data can flow from the 25 EU member states and three EEA member countries to that third country without any further safeguard being necessary. The Commission has so far recognized Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe harbour Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

2.1 Harmonisation or confusion

Prima facie the directive has had a harmonising impact in that it has led to the adoption of legislative measures in other countries, e.g. the USA has adopted a 'safe harbor' scheme whereby US bodies are able to qualify as offering adequate protection for personal data flowing from the EU/EEA by voluntarily adhering to a set of basic

[7] Regulation (EC) 45/2001 of the European Parliament and of the Council of 18.12.2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (OJ L 8. 12.01.2001)

[8] Art 286 (1) of 1957 Treaty establishing the European Community. The requirements of Art 286 are given effect by Regulation (EC) 45/2001 of the European Parliament and of the Council of 18.12.2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.

[9] The adoption of a (comitology) Commission decision based on Article 25.6 of the Directive involves: (1) A proposal from the Commission, (2) an opinion of the group of the national data protection commissioners (Article 29 working party), (3) An opinion of the Article 31 Management committee delivered by a qualified majority of Member States, (4) A thirty-day right of scrutiny for the European Parliament, to check if the Commission has used its executing powers correctly. The EP may, if it considers it appropriate, issue a recommendation, (5) The adoption of the decision by the College of Commissioners.

data protection principles.[10] However, scholars have expressed doubts about its suitability for regulating data flows to third countries, as well as its likelihood of success.[11] Moreover, in 2001 the EU Working Party concluded that Australia's legislation was inadequate because exemptions from the privacy regime for small businesses were considered too broad, whilst exemptions for employee information were regarded as potentially sensitive.[12] The Attorney General rejected the Working Party's findings on the basis that they "display an ignorance about Australia's law and practice".[13] Thus the directive has been controversial in its interpretation and implementation.

Furthermore, the impact of the adequacy rule is significantly mitigated by a set of derogations in Art 26. These derogations permit transfer of personal data to a third country lacking adequate protection if the proposed transfer: occurs with the consent of the data subject, or is necessary for performing a contract between the data subject and the controller, or a contract concluded in the data subject's interest between the controller and a third party, or is required on important public interest grounds, or is necessary for defending legal claims, or is necessary for protecting the data subject's final interests, or is made from a register of publicly available information. (Art 26(1)). A further derogation is permitted if the proposed transfer is accompanied by 'adequate safeguards' instigated by the controller for protecting the privacy and other fundamental rights of the data subject (Art 26(2)). The provision also states that 'such safeguards may…result from appropriate contractual clauses.' The EC Commission has the power to make binding determinations of what constitutes 'adequate safeguards' Art 26(4). It has exercised this power by stipulating standard contractual clauses that may be used to govern the transfer to third countries that do not offer an

[10] As of 09.03.2006 894 organisations had signed up to the scheme <http://web.ita.doc.gov/safeharbor/shlist.nsf>

[11] Reidenberg, J. R. (2001) "E-Commerce and Trans-Atlantic Privacy" 38 Houston Law Review 717, 740 ff. He criticised the legality and utility of the scheme. Also, EC Commission Staff Working Paper on the application of the scheme found evidence that organisations were failing to abide by the scheme rules <http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf> (Brussels, 12.02.2002, SEC (2002) 196).

[12] It also criticised the privacy regime because: NPP 2.1(g) allows use or disclosure where required by law. NPP 1 allows collection through a third party. NPPs 1 and 2 allow collection for secondary purposes in some circumstances. NPP 10 regulates collection but not use or disclosure of sensitive information (except for health information). NPP 9 allows the transfer of information from Australia to countries without adequate privacy laws. The definition of *generally available publication* is inappropriate.<http://www.aar.com.au/privacy/over/data.htm>

[13] <http://www.ag.gov.au/www/attorneygeneralHome.nsf/Web+Pages/8C9464056CE8169CCA256B5A001318DF?OpenDocument >

adequate level of data protection.[14] As a result, some third countries have not yet implemented data protection; rather, they have relied on contractual arrangements to govern their transactions. One such example is India. Given the huge growth in outsourcing work by Indian firms this may appear surprising, but is explained by reference to societal and economic conditions

> "the focus seems to be on meeting the external business needs. In India many people freely give their personal data without awareness of how it will be used and without any awareness of a need for concern. They have more pressing needs…This is a challenge for the government as there is no public call for data protection laws, and so they have to decide whether to introduce laws that will apply solely to foreign data or extend to domestic data subjects which will be a further burden on this developing economy… The lack of data protection law is not preventing business, but it is embarrassing to admit that we still don't have legislation…it's just not a legislative priority as there is no great political pressure from the public on politicians to push the legislation through…industry is weakening its position in an attempt to gain something, anything…"

Thus, although the directive seeks to ensure that the global village is governed by similar rules, to date, patchy implementation in non EU countries suggests that harmonisation is much more apparent than real. At this juncture it is appropriate to explore whether there is a harmonious understanding and implementation of key underlying concepts, namely personal and sensitive data.

3. Concept of Personal data

Art 2 (a) of the Directive states personal data:

> "shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[14] Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC (O.J. 181. 04.07.2001, 19); Decision 2002/16/EC on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (O. J. 10.01.2002, 52)

3.1 Differences in implementation

3.1.1 A distinction between data and information

No jurisdictions reported any difficulty in defining or interpreting the terms 'data' or 'information'.[15] The law in the UK makes a formal distinction between the terms. However, research by Kroff[16] indicates that in practice it has had little effect. Despite the apparent similarities between the formal definitions described, the Data Protection Authorities demonstrates a lack of consistency at the level of operationalisation of the concept 'personal data'. For the majority of data types, there seems to be a consensus that it *is capable* of being personal data but there is some dispute as to whether this occurs in all or only some circumstances, for example, 'national registration number' received the highest proportion of 'always' considered personal data classifications (78%) whereas shoe size and death details received the lowest proportion of 'always' classifications (33% in each case). The only consensus was a reluctance to state that a piece of data can *never* be personal data.[17]

3.1.2 Natural Person

In the UK and Ireland, data must relate to a 'living' person – once a person has died, their rights under the legislation cease. Also, the definition only applies to individuals, so a database containing names and addresses of limited companies would not be caught, whereas such a databank also containing names of company officers or employees would fall within the definition because a living individual could be identified by their name and workplace. Additionally, where a data controller possesses two databases then, provided an individual could be identified from the combined information of both databases, the relevant content of each amounts to personal data, even if an individual could to be identified from only one of the sources. The legislation also applies to encrypted databases.[18] It is interesting to note that the definition of personal data in the UK legislation is narrower than the EU

[15] Booth, S., Jenkins, R., Moxon, D., Semmens, N., Spencer, C., Taylor, M. & Townend (2004) "What are 'Personal Data' ? : A study conducted for the UK Information Commissioner"
[16] Korrf, D. (2002) EC Study on the Implementation of Data Protection Directive, Comparative study of national laws
[17] Booth et al,
[18] for further details, Carey, P. (2004) Data Protection: A practical Guide to UK and EU Law, Oxford University Press, 15

Directive[19] as the UK law refers to 'identified' whereas the directive refers to 'identifiable' and would potentially exclude the processing of a CCTV image where a specific individual could not be identified by name from the image. However, as a matter of law the UK Act must be interpreted to give effect to the Directive.

The law in Finland expressly states that it applies not just to information on an individual, but also to information on a family or household. Similarly Guernsey reported

> "It is important to explore the concept of family data. In Asian cultures it is normal for all family members to know information about each other to a greater extent that you find in British culture. Their family knows everything about them. Family has a higher status than the individual. An example is a Pakistani Muslim immigrant in the UK who falls pregnant at 15yrs of age. Her family believe they have the right to know all the details surrounding the pregnancy e.g. from medical sources as the rights of the individual are subjugated to wider family issues. Likewise in Chinese cultures the individual's rights are subjugated to family."[20]

An alternative approach is adopted in the laws of Austria, Italy and Luxembourg, which extend the concept of data subject to legal persons.

3.1.3 "Relating to… can be identified, directly or indirectly"

Korff opines that the definition of personal data contained in the Directive can be read as being 'relative'. Thus, the way that this phrase is interpreted influences what is or is not classed as personal data. Firstly, if interpreted very narrowly, it can be restricted to data that is capable of identifying an individual either by itself or in combination with other data. The advantage of this approach is that encoded data is

[19] "Personal data shall mean 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 to one or more factors specific to his physical, psychological, mental economic, cultural or social identity."

[20] Mc Cullagh, K (2005) Ongoing research. 25 Interviews have been conducted to date with a sample of those who have a professional interest in privacy and data protection, including commissioners, ombudsmen, lawyers, industry experts and academics, in a range of countries. The countries can be divided into three groups for the purposes of analysis: Group 1 - EU jurisdictions & the three EEA countries. Group 2 – Non-EU countries that have 'adequate' data protection compatible with EU legislation for trade purposes (under Article 25(6) of the Directive). Group 3 - countries outside the EU with no requirement of compatibility. Semi-structured interviews were used to explore understanding and satisfaction with current definitions personal data and sensitive data.

included. Belgium has adopted detailed rules on the processing for research purposes of fully identifiable, encoded, pseudo-anonymised and fully anonymised data. Accordingly, Rouille-Mirza and Wright argue that

> "…For data to be ever fully anonymous there can be no instance anywhere in the country or even the world, where information that can be used to link anonymised data to the individual exists". [21]

They suggest that 'Indirect' Identification,' where an individual could be identified from the data or the data and other data, can only be made workable by a concept of reasonableness, and Recital 26 provides a potential 'practical solution' to define the limits of indirect identification.[22] The laws in Denmark, Finland, France, Italy, Spain and Sweden are ambiguous in this respect, but the authorities tend to agree with the Belgian approach, and in principle, regard all data which still can be linked to an individual as 'personal,' even if the data are processed by someone who cannot make that link. However, they are willing to be flexible with regard to the processing of not-immediately-identifiable data, in that the question of whether the law applies, and if so, to what extent and how strictly is related to the probability of the data subject being identified, with the nature of the data also being taken into account. The more sensitive the data, the closer the data protection authority will examine the likelihood of the data becoming identifiable, and thus the need to apply the law.[23]

Alternatively, the term 'can' could refer to the capabilities of a person or organisation that might have access to the data: the data are then "personal" for a person or organisation which 'can' link the data to an identified individual, but not for someone who cannot establish such a link. The second approach has the advantage that it does not extend duties to persons and organisations that have neither intention of, nor capability of, linking it to specific individuals. The laws in Austria, Germany, Greece, the Netherlands and the UK make clear that, encoded or pseudonymised data are to be regarded as 'personal' with regard to a person who has access to both the data and the 'key,' but not as such with regard to a person without access to the 'key' (the Austrian law refers to such data as 'indirectly identifiable data,' while other laws

[21] Rouille – Mirza, J. & Wright, J. (2003) PRIVIREAL Issue Paper s1. 1.2
[22] *ibid*
[23] Korrf, (2002) 15

add separate definitions of pseudonymised data, etc). The term "personal data" is also regarded as relative in Portugal. In Ireland, the data protection authority takes into account the likelihood of a particular person being able to identify a person from data in his or her possession.

The two approaches are more consistent if one takes into account that the act of anonymising of data itself constitutes processing. This means that a controller who intends to disclose encoded data must fulfil the requirements for lawful processing. Thus, in Portugal, prior consent is required for the encoding of sensitive data intended to be disclosed in encoded form for scientific research, even though the data once disclosed in that form are not regarded as 'personal.' In Durant v FSA [2003][24] the UK Court of Appeal considered identified two notions that may assist in determining whether information 'is information that affects [an individual's] privacy':

> "The first is whether the information is biographical in a significant sense, that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations…"

The second concerns focus.

> "The information should have the [individual] 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 …"

The Court did not consider the issue of the identifiability of an individual in the definition of 'personal data' set out in section 1(1) of the Data Protection Act, instead it concentrated on the meaning of 'relate to' in that definition. 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[25] or information regarding his hobbies.[26] Also, the term 'relating

[24] EWCA Civ 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003

[25] See European Court of Justice decision in Bodil Lindqvist v Kammaraklagaren (2003) C-101/01, paragraph 27, as referred to in paragraph 28 of the Durant judgment

[26] See Lindqvist case (see above), paragraph 27, and Durant at paragraph 28

to' has been associated with a meaning that extends beyond simple 'identification'. Auld LJ stated that

> "not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his 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."[27]

Clearly, this is a reading of 'relating to' that requires something more than mere identification for data to be classed as personal. One respondent said they wouldn't consider workplace or product data as personal following the Durant case. The example given was

> "If you produce a report at work you are the author. This might be considered personal data under the EU Directive, but is unlikely to be considered personal data after Durant"[28]

The issue is related to the use of data that relate to an object which relates to a person, such as a car, or a house, or a personal computer. Sometimes, the relationship between an object and its owner or registered keeper is so close that the data on the object are invariably regarded as data on the person: data on car licence plates, and IP-addresses linked to a particular PC are thus everywhere treated as personal data. In other contexts, the issue is less clear. Thus, for instance, most people would agree that a photograph of a street with houses (and not showing people) does not contain personal data. However, a systematic collection of such photographs, with links to individual owners or occupiers would constitute such data. Thus, postcode or statistical data by their nature do not relate to particular individuals but to a group of individuals. Yet, if one applies such statistics to an individual, they do become

[27] EWCA Civ 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003
[28] Mc Cullagh

'personal data' e.g. if one takes such statistics into account in deciding on credit limits; or in excluding people from a list of applicants for a job.[29]

The findings from previous studies are confirmed by responses in interviews conducted with privacy and data protection experts.[30] 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, whilst 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. click-stream data of linked sites can lead to a profile being created which may or may not be considered personal data.

4. Concept of Sensitive data

EU Directive 95/46/EC defines sensitive data in Article 8 (1) as:

> "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

Very stringent rules apply to processing sensitive data. The principle holds that the processing of certain types of data which are regarded as especially sensitive for data subjects, should be subject to more stringent controls than other personal data. In principle, such data cannot be processed. Derogation is tolerated under very specific circumstances.[31]

[29] Korrf, D. (2002) 17

[30] Mc Cullagh (5005) Ongoing research

[31] These circumstances include the data subject's explicit consent to process sensitive data, the processing of data 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.

4.1 Differences in implementation

Korrf [32] conducted a comparative textual analysis of legislation. He found that *prima facie* most Member States had adopted the categories of sensitive data listed in the Directive. Mc Cullagh found that some respondents were happy with the existing definition and the types of data covered. For instance, in Ireland

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

Others expressed a view that they did not agree with all classifications. Indeed, attempts to delineate particular categories of data for special protection have been controversial. For instance, in Denmark, information on a person's trade-union membership was not regarded as "sensitive" until the Directive stipulated this. Likewise in Iceland

> "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. … We should have differentiations in the definition of sensitive data e.g. some health data is less sensitive than financial data e.g. the fact I had flu last week is less sensitive than how much pay I take home".

An important issue is whether Art 8(1) categories are exhaustive. Some claim that the list is exhaustive,[33] others disagree, primarily due to the subsequent inclusion of data

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

[33] Blume, 432 cited in Bygrave, (2002) 344 Declaration 11 of Council minutes indicate that the intention of both the Council and Commission was that member states, in light of their respective legal and social circumstances could specify categories that are an elaboration of the categories in Art 8(1) e.g. data relating to genetic identity, party political membership, physical health personal persuasion, lifestyle etc.), but that states could not introduce totally new categories.

relating to criminal convictions in Art 8(5).[34] Moreover, Korrf noted that several countries impose special restrictions on certain categories of data, which are not formally included in the list of "sensitive data" in Art 8(1) of the Directive. Thus data on matters such as creditworthiness or debts are subject to special restrictions in Denmark, Finland, Greece, the Netherlands and Portugal. In France, such data are regarded as subject to *special obligations of confidentiality* (in particular when processed by financial institutions), and subject to strict scrutiny, in particular as regards *disclosures* and\or *secondary uses*.[35] Whereas, in Spain a different approach is advocated

> "Financial information is not sensitive. This is not a problem area in Spain. 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".

Further divergences arise from the fact that some laws contain additional categories. For example, Finnish law treats data on "*social affiliation*", "*treatment*" and "*social welfare benefits*" as sensitive; and Greece regards *membership in* any *association* and data on "*social welfare*" as sensitive. In Luxembourg, the Netherlands and in Portugal, genetic data are defined as *health and sex life data*, while in Sweden the processing of such data is separately regulated. Consequently, during interviews with Mc Cullagh some Interviewees suggested new categories of sensitive data. Below are some illustrations:

> "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. They could be expanded e.g. to include financial data. They could be ramified, e.g. for health data a biometric template should

[34] Bainbridge, D., & Pearce, G. (1996) "The Data Protection Directive: A Legal Analysis" 12 CLSR, 160, 163
[35] Korrf, D(2002) 86

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. Technology is creating new issues. We may need to develop a concept of "supersensitive" data, which is subject to stricter tests. E.g. behavioural/click-stream data could be supersensitive. For instance if there are two parties to a transaction the counter-party may expect commercial value. This is a controversial idea. Anonymity technologies might be appropriate for such circumstances. If well designed they can use alarms to trigger identification when the rule is breached – otherwise processing of the information would be anonymous, so it would facilitate conditional anonymity."

"We conducted a review of the enquiries and complaints at issue in our Australia office a few years ago. Health information was top of the list. A close second was personal contact details, even though it is not considered sensitive under the Act. Financial information is not highly nominated in surveys – perhaps because it is not really abused. I'd take out trade union membership, as although I can see how it might be misused, in our society it is not generally regarded as sensitive. I would include criminal record/history, contact details and financial information in a definition of sensitive information."

5. Concluding remarks

In summary, whilst the global village is now governed by similar personal data protection rules harmonisation remains more apparent than real as the preceding analysis indicates that the definitions used do not lead to a uniform understanding of the key concepts underpinning the directive. The Directive was intended to create a harmonious European wide system of data protection whilst simultaneously supporting the single market. It potentially exerts political and legal influence in countries outside the EU through trade negotiations, in that it prohibits the transfer of personal data to these countries unless they provide 'adequate' levels of protection. However, to date, patchy implementation of adequate legislation in non-EU countries suggests that harmonisation remains a distant goal.

Although all respondents were familiar with the concept of personal data and sensitive data and had knowledge of the EU Directive 95/46/EC or it had been implemented into their national legislation, research by Booth *et al*, Korff, and Mc Cullagh confirms that, the way in which the Directive has been implemented has created divergences both between Member States' laws and in the ways they are applied in practice. Some respondents were happy with the existing definitions and the types of personal data covered. Others expressed a view that they did not agree with all classifications. Some discussed the fact that technological developments are causing difficulties

> "The accelerating pace of technological development is important. Data storage is so cheap and the value of personal data to an individual is so high that there are many reasons for an individual wanting to have a complete life record. The issue is whether that data can remain under the control of the individual or family unit?… A hot future issue will be the convergence of key escrow and data retention as undoubtedly Law enforcement agencies will want access to the data…At present there is no political will for law enforcement transparency – in the UK oversight is provided by retired judges. But, how can they be effective in overseeing when they have to rely on agency information?"

It is suggested that the time is ripe to review the provisions of the directive. Some Interviewees suggested new categories of sensitive data. The current definitions reflect post World War II concerns regarding discrimination and protection of human dignity, but it may be that in the 21st century new concerns are arising due to technological developments. However, a decision to simply include new categories, or delete existing categories should not be taken lightly. It is suggested that 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[36] 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

[36] 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

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

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

In concurrence with Simitis[37] it is suggested that sensitivity of data varies from context to context. Moreover, Wacks[38] 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. Thus, lessons may be learned from reviewing the approach taken by other legislatures

> "Canadian law has a concept of sensitive data, but the approach taken differs from the EU concept of sensitive data. It can be used as an interpretative aid to explain why it is necessary to reveal certain information. Sensitivity depends upon 2 criteria: 1) the point of view of the data subject, 2) the context in which a 3rd party uses the data. Very little data has an absolute character. The Canadian definition can be adapted to reflect information that the data subject wishes to control."

Categorisation of sensitive data should be understood as an indicative flexible, reference list. Legislators should regularly review the list in view of experiences of data subjects and data processors and new technological developments.

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

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