TECHNICAL
REPORT

Review of the European Data Protection Directive

Neil Robinson, Hans Graux,
Maarten Botterman, Lorenzo Valeri

RAND EUROPE

TECHNICAL
REPORT

Review of the European Data Protection Directive

Neil Robinson, Hans Graux,
Maarten Botterman, Lorenzo Valeri

Sponsored by the Information Commissioner's Office

RAND EUROPE

The views expressed in this study are those of the authors and do not necessarily reflect those of the Information Commissioner's Office.

Published 2009 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org/
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Review of the European Data Protection Directive

NEIL ROBINSON, HANS GRAUX,
MAARTEN BOTTERMAN &
LORENZO VALERI

TR-710-ICO

May 2009

Prepared for the Information Commissioner's Office

Preface

The Information Commissioner's Office (ICO) asked a multidisciplinary international research team led by RAND Europe with time-lex and GNKS-Consult to review the strengths and weaknesses of the European Data Protection Directive 95/46/EC and propose avenues for improvement. Soon after the ICO requested this review, the European Commission (EC) published its own request for a similar study.

The Directive can be regarded as a unique legal instrument in how it supports the exercise of a right to privacy and rules for personal data protection. Its principles are regarded in many quarters as a gold standard or reference model for personal data protection in Europe and beyond. However, the Directive must remain valid in the face of new challenges, including globalisation, the ongoing march of technological capability and the changing ways that personal data is used. Although the flexibility of the Directive helps it to remain current, its effectiveness is undermined by the complexity of the cultural and national differences across which it must operate.

In order to understand the strengths and weaknesses of the Directive and to suggest ways in which European data protection arrangements may remain fit for purpose, the study team reviewed the relevant literature, conducted 50 interviews with privacy practitioners and regulators, experts and academics, and ran a scenario-based workshop to explore and evaluate potential avenues for improvement.

The ideas presented here provide some food for thought on how to improve the data protection regime for citizens living in European countries and are intended to spark debate and interaction between policy-makers, industry and experts. Given the complexities of European policy-making, such a review cannot claim to be the last word.

For more information about RAND Europe or this document, please contact

Neil Robinson
RAND Europe
Westbrook Centre
Milton Road
Cambridge
CB5 1YG
+44(0)1223 353329

Acknowledgements

The authors would like to express their gratitude to Constantijn van Oranje, Simone Vernacchia, Kate Kirk and all those who gave of their time to review the various drafts of this report.

Contents

Summary

Objective of the study

In April 2008, the Information Commissioner's Office (ICO) commissioned a review of the 1995 EU Data Protection Directive (95/46/EC, hereafter "the Directive"). In the 13 years since the Directive came into force, the world has seen dramatic changes in the way personal data is accessed, processed and used. At the same time, the general public has become increasingly aware of the potential for their personal data to be abused. Through this study, the ICO wishes to examine if the Directive is still an effective tool for the protection of personal data, and what possible advantages could be gained through any alternative approaches.

Research Approach

Using a variety of research methods, including a review of relevant literature, interviews with 50 individuals and a scenario-based workshop, we examined the strengths and weaknesses of the Directive and its current application in practice.

Overall conclusion

Overall, we found that as we move toward a globally networked society, the Directive as it stands will not suffice in the long term. While the widely applauded principles of the Directive will remain as a useful front-end, they will need to be supported by a harms-based back-end in order to cope with the growing challenge of globalisation and international data flows. However, it was also widely recognised that more value can still be extracted from current arrangements. A lot can be achieved by better implementation of the current rules, for instance by establishing consensus over the interpretation of several key concepts and a possible shift in emphasis in the interpretation of others. Abandoning the Directive as it currently stands is widely (although not unanimously) seen as the worst option, as it has served, and continues to serve, as a stimulus to taking data protection seriously.

This overall vision is reflected in the report you are about to read. Based on our findings, we have formulated recommendations in line with this evidence.

Context

The privacy of individuals is affected by a number of intersecting drivers, including the need to process personal information for social and economic reasons, technological developments and trends such as the popularity of the Internet and globalisation. The delivery of e-Commerce and e-Government are becoming centred on personal information.

Individuals are often willing or can be persuaded to give out personal data in the expectation of receiving economic or societal benefits. Public and private sector organisations are happy to provide individuals with these benefits but, in order to do so, must be permitted to legitimately collect, transfer and process the information. Individuals have also started to collect, manage and use personal data in similar ways, for example through social networking sites.

Against this background, it seems that the impact of the Directive on European perceptions of data protection principles has been largely positive. It can be credited with harmonising and professionalising the main data protection principles within Europe, even if implementation still varies, as will be explored below. The Directive can also be credited with creating one of the world's leading paradigms for privacy protection, which has served as an inspiration to legal regimes outside Europe.

However, despite this substantially positive track record and general acceptance of the sound principles behind the Directive, certain aspects have been criticised. Criticisms from within the EU have often focused on the formalities imposed by the Directive (or by the transpositions thereof), and the economic costs of compliance and unequal enforcement. Non-European organisations tend to perceive the European regulations as somewhat paternalistic towards other and perhaps equally valid data protection approaches.

The interviews conducted for this study illustrated that differences in implementation were the result of a complex interplay of factors, including legal heritage, cultural and historical norms and the personal and institutional characters of the regulatory authorities.

Challenges

Within the contexts of rapid technological change and globalisation, a set of distinct challenges were identified:

- Defining privacy – when is privacy affected by personal data processing and when is it not, and how strong should the link between data protection regulations and privacy protection be?
- Risk assessment – can we predict how risky it is to provide our personal data to an entity or organisation?
- The rights of the individual in relation to the benefit of society – under what circumstances can personal privacy become secondary to the needs of society, considering the fundamental importance of privacy protection for the development of a democratic society as a whole?

- Transparency – personal data is everywhere, particularly online, and through technological developments such as ambient intelligence and cloud computing could become increasingly difficult to track and control. How can we be sure how and where it is being used?
- Exercising choice – many services are only provided after sufficient personal data is released, but if important services are denied when we are unwilling to supply that data, do we still have a real choice?
- Assigning accountability –who is ultimately held responsible and where do we go to seek redress?

Strengths and Weaknesses

The study identified a number of strengths and weaknesses associated with the Directive. The main strengths were:

- The Directive serves as a reference model for good practice.
- The Directive harmonises data protection principles and to a certain extent enables an internal market for personal data.
- The principles-based framework permits flexibility.
- The Directive is technology neutral.
- The Directive has improved awareness of data protection concerns.

The main weaknesses identified were:

- The link between the concept of personal data and real privacy risks is unclear.
- The measures aimed at providing transparency of data processing through better information and notification are inconsistent and ineffective.
- The rules on data export and transfer to third countries are outmoded.
- The tools providing for transfer of data to third countries are cumbersome.
- The role of Data Protection Authorities (DPAs) in accountability and enforcement is inconsistent.
- The definition of entities involved in processing and managing personal data is simplistic and static.
- There are other minor weaknesses which add to difficulties in its practical implementation

Recommendations

Our recommendations stem from a broad (though not unanimous) recognition that although a lot can still be achieved in terms of better implementation and interpretation of

current arrangements, as we move toward an increasingly global networked environment the Directive will not suffice in the long term. In light of evidence collected during the course of the project, we have formulated a set of practical recommendations for getting the most out of current arrangements, along with a proposed regulatory architecture which we consider would be better suited for the future.

To extract the most out of the current system, we propose that:

- Member States, facilitated by the European Commission, need to seek agreement on efficient interpretation, implementation and enforcement of the Directive, including encouraging the use of a risk-based approach, making non-notification the general rule rather than the exception, ensuring that Binding Corporate Rules (BCRs) can be more easily used to legitimise data transfers to third countries, improving accountability and helping data processors meet transparency requirements.
- The European Commission should improve the effectiveness of the Adequacy Rule and facilitate the use of alternatives to this rule – such as standard contractual clauses and BCRs.
- The Directive should be explicitly included in the list of laws to be reviewed as part of the Better Regulation agenda.
- The Article 29 Working Party should work towards clarifying privacy norms and standards, the role of "privacy-by-design" for new technologies and business models that will foster compliance.
- The London Initiative should develop a common enforcement strategy for independent supervisory authorities through a non-binding Memorandum of Understanding.
- The Article 29 Working Party should expand liaisons with business representatives, civil society representatives and Non-Governmental Organisation communities.
- Data Protection Authorities, with guidance from the European Data Protection Supervisor (EDPS), should be encouraged to develop more accessible privacy policies e.g. comparable to the Creative Commons model for intellectual property rights licences.
- Member States should work with consumer protection related organisations to institute a system of local level accountability agents to help individuals exercise their rights and act as a means to prioritise workload for DPAs.

To make European governance architecture properly viable given international data flows, we also recommend that the upcoming 2009 Consultation considers an alternative proposed regulatory model, outlined below. This is based on:

1. Defining high level Outcomes
2. Defining globally consistent General Privacy Principles ("General Principles") based on well-known existing data protection instruments such as the European Charter on Human Rights and the 1981 Council of Europe Convention No. 108;
3. Implementing tools and instruments to achieve these, and
4. Foreseeing effective enforcement measures to ensure accountability when the Outcomes are not met or the Principles are not respected.

This will require the re-casting of the Directive to become an instrument clearly describing:

1. **Outcomes** in terms of expectations for stakeholders:
    - Individuals – to retain clear and effective safeguards whenever personal data is processed, including via accountability of the data controller, thus contributing to the protection of private life. To have the choice to exercise significant control over their personal data, including by sharing personal data with trusted third parties or withholding it from them, but to be mindful of the implications of this in an information society.
    - Public and private sector organisations – to be able to use personal data and derive economic or societal value as long as this remains aligned with the General Principles, in particular by processing data in line with the stated purposes, ensuring the legitimacy of their activities in accordance with applicable rules, and in the knowledge that they will be held accountable for non-compliance.
    - Independent Supervisory Authorities (ISAs) – to act independently and equitably across both public and private sectors, but to do so in a way that is mindful of the realities of the use of personal data. To use enforcement where necessary both to shape good behaviour and obtain restitution for any harm.

2. Globally consistent **General Principles** concerning privacy protection:
    - Legitimacy – defining when personal data processing is acceptable.
    - Purpose restriction – ensuring that personal data is only processed for the purposes for which it was collected, subject to further consent from the data subject.
    - Security and confidentiality – specifically by requiring the data controller to take appropriate technical and organisational measures.
    - Transparency – that appropriate levels of transparency are provided to data subjects.

- Data subject participation – ensuring that the data subjects can exercise their rights effectively.
- Accountability – that those processing personal data would be held accountable for their actions according to the Outcomes.

The implementation or 'back-end' aspects, i.e. the processes to ensure that these General Principles are respected, should be delivered by other more suitable means, which may need to be created or defined by formal EU level implementing measures or locally at the national level. The selection of appropriate means for specific acts of data processing can be determined locally, either via national data protection rules (generic or sector/context specific) or via co-regulation (e.g. established via dialogue between ISAs and sectoral representatives). This selection should be based on considerations of risk, with more burdensome tools being used only when this is justified by the risk presented by specific acts of data processing.

Further discussion will be required to clarify how regulation can appropriately consider and address the presence of risk. Possible criteria or avenues for determining the risk involved in specific categories or acts of data processing include:

- the scale on which personal data is processed (e.g. more stringent requirements could be applied to the processing of personal data based on numbers of data subjects involved);
- the privacy sensitive nature of the data being processed, and more specifically whether the nature of this data causes it to be more likely to result in harm, considering the full context of the data processing (e.g. the processing of health-related information, racial information, etc) and
- the field of activity of the data controller, as a proxy for the risk of harm (e.g. financial services, health care, legal services).

While risk is often difficult to determine ex ante, the strength of a risk-based approach lies precisely in the need to evaluate how risk changes dynamically as data processing practices evolve (e.g. because of changes in the scale of data processing, or expansions to other fields of business). As practices change (and as risk changes), the measures needed to ensure compliance will evolve as well. In this way, a risk-based approach stresses the importance of implementing a sound data protection culture, rather than meeting one-off compliance formalities.

The need to appropriately consider risk as the predominant consideration in determining in what way the fundamental right to the protection of personal data as specified in the European Charter of Fundamental Rights may be best safeguarded supports this right without the imposition of inappropriate or disproportionate burdens. A risk based approach should thus not be interpreted as arguing for the application of regulations only when there is a sufficient risk of harm.

Data protection practices can thus be assessed on the basis of whether the desired Outcomes and General Principles are met, rather than on the basis of a process orientated review. Mutual acceptance of different instruments as viable routes to achieving the Principles and Outcomes would be required to mitigate the risk of fragmentation of the

internal market (for instance, by one ISA refusing to accept an instrument considered as valid by another).

3. **Implementation measures** would include:
    - Privacy policies – internally focused tools describing how an organisation intends to achieve the principles set out above and a clear means to provide for accountability.
    - Privacy notices / statements – externally facing tools supporting objectives of transparency, these would alert individuals at an appropriate time and context as to how their personal data is being used.
    - Chief Privacy Officers – this role may be identified as an alternative to a privacy policy, there mainly to provide for accountability within an organisation.
    - Codes of Conduct – self-regulatory tools defining the common rules for similar types of organisation.
    - Corporate Governance Codes – developed and published by the regulator, these might be non-binding set of rules for organisations to follow, where they must comply or explain why they do not.
    - Privacy Reporting / Accounts – based on the likely risk, organisations might be compelled to produce data reflecting their use and incidents relating to personal information.
    - Standards – providing for another aspect of accountability by allowing regular external review of processes and policies by third parties to ensure the organisation is living up to its own rules.
    - Kite-marks / Trustmarks / Seals – a way for consumers to exercise their rights as an enabler of choice between those organisations that display a trust mark and those that do not.
    - Privacy Impact Assessments – a way to assess a-priori the impact of certain measures upon individuals' privacy, formal and informal methods of conducting Privacy Impact Assessments support the same purpose of encouraging responsibility and respecting proportionality.
    - Technology – a way to enforce policies or support compliance, technology may be used appropriately in the context of the greater objectives of the achievement of Outcomes by satisfying General Principles.
    - Targeted information campaigns – to increase understanding of risks and issues regarding the use of personal data amongst individuals and public and private sectors.

Some of these tools will be more appropriate for either public or private sectors and ISAs might establish mandatory uses of some instruments for the public sector. The public sector might also be able to set an example in adoption of various instruments.

National legislation, along with cultural and political conditions, will play an important role in the implementation of these tools in the public sector.

4. To support these tools, **enforcement** will be necessary. ISAs must be able to intervene when misuse has been identified, either pre-emptively, or after the fact when actual harm has occurred. In order to ensure effective and credible enforcement:
    - Possible liabilities, sanctions and temporary measures should be clearly published.
    - Criteria for determining fines should consider risk –for example, numbers of personal records involved, whether the incident involved actual harm, and if so, what sort of harm.
    - Criminal sanctions may be considered for serious incidents or intentional misuse, to act as a deterrent and punishment.
    - Alternative Dispute Resolution may also be considered, to permit easy and quick access to restitution or compensation in low level cases of misuse.
    - Efficient enforcement can be improved through strategic partnerships and joint enforcement efforts between ISAs and consumer protection bodies, especially in countries where there is a stronger culture of consumer protection. This will improve coherence in protecting the individual, and will encourage compliance with data protection regulations to evolve into an economic differentiator.
    - Ultimately, ISAs will need to act more strategically to achieve real outcomes rather than meeting targets for completed investigations.

All this indicates that ISAs, those organisations using personal data and individuals will need to assume greater responsibility for achieving the Outcomes. For their part, ISAs will need to adopt an approach that is less focused upon process and formality checking, but instead aims for more effective enforcement and ensuring accountability. Those using personal data will need to assume responsibility for making sure the measures they select to achieve the Outcomes are consistent with the level of risk that personal data is exposed to by their business activities. Individuals must also take more responsibility in the choices they make with their personal data.

The research for this study showed clearly that the success or failure of privacy protection is not principally governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work.

Introduction

Defining privacy

Our current understanding of informational privacy is based to some extent on how an individual relates to and controls access to information about themselves. Regulations and legislation have codified what Judge Samuel Warren and Louis Brandeis summarised in 1890 as the right of the individual to "be let alone"[1], and expanded the notion of data protection beyond the fundamental right to privacy. Warren and Brandeis were writing on a court case in which the then new technology of photography had been used to collect data and information about an individual without their consent. Technology, particularly Information and Communications Technology (ICT), has evolved considerably since then, but the basic concept of privacy is still valid. As an ideal, an individual should be able to decide (with a few exceptions) between being open or to remain, as described by Professor Alan Westin, in "solitude, intimacy, anonymity, reserve".[2] Others such as Solove have indicated the complexity of defining privacy, admitting it is a "conceptual jungle"[3] and instead proposing a more nuanced definition, decoupling privacy from a fundamental human rights approach based on how privacy is understood in the context of solving certain problems.[4]

Privacy is recognised as a fundamental human right by various legal instruments, including the Universal Declaration of Human Rights (UN, 1948) and the European Convention on Human Rights (ECHR, Council of Europe, 1950). Privacy regulations aimed at governing how personal data is processed were introduced in the 1970s and 1980s, and the European Data Protection Directive came into force in 1995.

The various national and international normative instruments are based on a set of conditions or principles that include:

- Individuals should be informed when personal data is collected.

---

[1] Warren, S.D and Brandeis, L.D. The Right to Privacy *Harvard Law Review* Boston Vol. IV No. 5 Dec 15; 1890

[2] Westin, A; *Privacy and Freedom* New York NY, Atheneum 1967

[3] Solove, D.J., *Understanding Privacy* Harvard University Press 2008 p196

[4] See generally Solove, D.J., *Understanding Privacy* Harvard University Press 2008

- Individuals should be told who is requesting the data and the reason for their request to help them decide whether to release control of all or part of such data.
- Individuals should be told how they can access data about themselves in order to verify its accuracy and request changes.
- Individuals should be told how their data will be protected from misuse.

Implementing these conditions is not easy, particularly in today's world, where personal data is collected, processed and transferred in vast amounts, either on behalf of the individuals themselves (e.g. by the state to preserve security or improve public services) or for the benefit of commercial organisations. In such an environment, these principles must be observed in an effective way, guaranteeing the respect of the data subject's rights without overloading him with formal information in quantities that he cannot realistically be expected to process or comprehend.

Risks, harms and damages to privacy

Identifying damage or the resulting harm when privacy protections are removed or breached is a complex task. There may be direct and indirect forms of damage and they may have consequences upon the individual in a variety of ways, ranging from monetary to social, mental and physical. It is also difficult to identify types of harm in advance. Finally, loss of privacy may also affect society at large, by undermining trust and confidence in those using personal data.

Van der Hoeven proposes a classification of four types of harm that may arise as a result of the compromise of privacy protections:[5]

- Information based harm – of which the obvious types are identity theft but which also may include harms to the person, which are only possible following the acquisition of data or information about the person. In the information society, the prime examples are identity theft (according to the Home Office the cost of identity theft to the United Kingdom economy was £1.7bn[6]).
- Information inequality – where information about purchases and preferences are used for the purpose of marketing, price discrimination without awareness on the part of the individual or being able to influence this process. The use of behavioural monitoring and analysis techniques is a case in point in this instance – where based on information about past purchases or habits, the same goods and services may be offered at different prices. Furthermore, this may lead to discrimination where individuals or certain social groups are singled out for adverse treatment on the basis of misleading or incorrect assumptions.

---

[5] Hoven, Jvd. Information Technology, Privacy and the Protection of Personal Data in Weckert, J., Hoven, Jvd.; (eds) *Information Technology and Moral Philosophy* Cambridge University Press 2008 p 311

[6] The lack of European data on identity theft was criticised in a recent scoping paper for the OECD Future Internet Conference see; Acoca, B.; *Scoping Paper on Online Identity Theft*, DSTI/CP(2007)3/FINAL, OECD, 2007 p6

- Information injustice – where information presented in one context is used in another. A good example is where prospective employers have begun to search Social Networking Sites (SNS) for personal information on job candidates. Other examples include the mistaken detention on the basis of erroneous or inaccurate personal information, as occurred with the US lawyer Brandon Mayfield who was imprisoned for two weeks by the US Federal Bureau of Investigation (FBI) in June 2004 following a match between his fingerprints with those found in the Madrid terrorist bombing.[7]
- Restriction of moral autonomy – where people are restricted or limited in their options for self-representation due to the omnipresence and pervasiveness of personal information. This may also be termed a restriction on the choices that the right to privacy protects. An example of this can be seen in behavioural profiling and advertising where persistent profiles may exist across a number of different domains, or in the creation of multiple on-line personas as a response to the need to keep personal data contexts clearly separate (e.g. one profile for friends, one for acquaintances, one for professional use).[8]

Each of these types of harm may directly or indirectly affect individuals. Indirectly, they may cause tensions or destroy relationships because of the exposition of personal data. Individuals may live in fear that others are seeking to use their personal data to cause them harm, for instance in cases of stalking or personal surveillance. There may be direct impacts, too – for example via credit card fraud, physical harm or lost possessions.

It is also worth considering the broader consequences of the way in which personal data is being used. Whilst it may be possible to identify specific cases of harm for an individual in physical or financial terms, there are also societal consequences which may arise from the persistent and systemic pressure for the acquisition and use of personal data. Indirect societal impacts may include the creation of a climate of fear or distrust or a loss in confidence in those organisations using personal data. This was seen with recent large scale data losses in the United Kingdom, for example. It is much more complex, however to define societal harms consistently across national boundaries, since what may be seen as acceptable in one nation may not be so in another. A good example is in perceptions of privacy in other nations and cultures across the globe where privacy is determined more in physical than informational terms.

Finally, it is worth noting that fully understanding the question of harm raises some important philosophical issues. Esther Dyson points out that it is possible to distinguish objective harms (denial of a service, fraud) from subjective privacy harms (knowledge by a second or third person is experienced as an injury). She also highlights a concern that reflections on privacy may actually be matters of security health policy insurance or self-

---

[7] Wax, S.T. and Schatz, C., J., *A Multitude of Errors: The Brandon Mayfield Case* National Association of Criminal Defense Lawyers available at: http://www.nacdl.org/public.nsf/0/9090373de4fa9c7d85256f3300551e42?OpenDocument

[8] See e.g. Thompson, C.; "Brave New World of Digital Intimacy', *New York Times*, 5 September 2008, http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html?_r=3&oref=slogin&partner=rssuserland&emc=rss&pagewanted=all&oref=slogin

presentation. For example, in the US with its private healthcare system, people would not feel a need to keep their personal medical data private if they thought that exposing it would not result in discrimination, expensive bills and higher insurance premiums. In reality this might mean deciding what forms of discrimination are acceptable in the information society.[9]

The individual perspective

Individuals generally do not systematically undertake a considered balancing of their rights or what is permissible when considering the importance of their own privacy. At a pragmatic level, they may choose or be required to surrender their personal information in order to obtain benefits in exchange, for instance providing information when buying goods online. Society may also decide through specific regulations that certain individuals within certain contexts may have parts of their right to privacy abrogated for law enforcement or national security reasons, e.g. in the course of criminal investigations or intelligence operations to avert potentially more harmful damage to society from public security risks.

Privacy (and the impact of its loss) is of course extremely context dependent. Taken out of context, something that could be considered harmless personal data might be used to cause harm if combined with other personal or non-personal data. Managing this is thus not a task that an individual can succeed in alone, but rather must engage with and rely upon other third parties (either regulators or organisations using their personal data) to meet expectations regarding the use of personal data and ensure that where possible it is not mis-used. Assessing the value of personal information is complex and also dependent on these contexts. For example, studies have discussed the value of credit card information on the underground 'black market'.[10]

Among consumers, there seems to be a growing and implicit understanding that the use of their personal data is intrinsic to the provision of most online and an increasing number of offline services.[11] This implicit and context bound acceptance should not permit their personal data to be distributed to other organisations, but it is difficult to establish in practice exactly how such information is being used or to set up any comprehensive means for individuals to exercise management or control of the uses of such data.

Consumers also have complex attitudes and behaviours when it comes to determining risk and harm. Research has shown that they tend to value losses twice as much as benefits,[12]

---

[9] Dyson, E.; How the Loss of Privacy May Mean the Loss of Security in *Scientific American* Special Edition on the 'End of Privacy?' August 2008 pp

[10] Anderson, R. Clayton R. and Moore, T.: *Security Economics and the Internal Market;* paper prepared for the Euroepan Network Information Security Agency 2008 available at: http://enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

[11] See the 2008 Eurobarometer results, published at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm; commented further below.

[12] Thaler, R. H., and Sunstein, C. R., *Nudge: Improving Decisions about Health, Wealth and Happiness* Yale University Press 2008 p 34

but that they are also prepared to gamble more with the chances of a loss than with a guaranteed loss.[13] From a data protection perspective, this same logic would imply that data subjects may be less likely to take precautions when managing their own personal data when the chances of data abuse or security incidents are unclear to them. If these risks are indeed difficult to assess a priori, it then follows that a suitable regulatory approach must also offer effective tools for individuals to act when such incidents occur, rather than focusing solely on defining data subjects' rights. Individuals may indeed change their behaviour if measures are put in place to deal with risks.[14] The literature on behavioural economics offers some interesting ideas in this respect.[15] One is that human decision-making exhibits bounded rationality, i.e. people cannot fully comprehend how their personal information might be used and so rely on tools such as rules of thumb and anchor points when making decisions.

Individuals also depend on some means of redress when things go wrong. This suggests the need for an authority or mechanism to establish accountability and take action when necessary.

[13] West R. The psychology of security: why do good users make bad decisions? *Communications of the ACM* April 2008 vol 51 No 4 pp 34 -40

Wilde, G.J.S. *Target Risk 2: A New Psychology of Safety and Health*, PDE Publications Toronto Ontario 2001

[15] See generally Part IV of Acquisti, A. Gritzalis, S. Lambrinoudakis, C. and di Vimercati, S (eds) *Digital Privacy: Theories, Technologies and Practices*; Auerbach Publications 2007

CHAPTER 1 The European Data Protection Directive

1.1 Historical context

At the European level, the protection of privacy as an essential human right has been encased in a number of regulatory texts, most of which came into being after the Second World War. The tragedies and atrocities of this period, when large databases of personal data were used to segregate populations, target minority groups and facilitate genocide, made it abundantly clear how dangerous it could be to allow public intrusion into the private sphere.

The post-war period witnessed the arrival of the Universal Declaration of Human Rights (UN, 1948), the European Convention on Human Rights (Council of Europe, 1950), and the International Covenant on Civil and Political Rights (UN, 1966), all of which recognised privacy as a fundamental human right and focused principally on shielding the individual against abuse by protecting their personal data.[16]

The private sector began to use personal data extensively following the arrival and broad uptake of Information, Communication Technology (ICT) in the 1970s. This increased the risk of personal data being abused and created concern that there would be a need for regulation to ensure that individuals remained adequately protected. Hence more specific regulations were introduced in the 1970s and 1980s to govern personal data processing, both at an international level (e.g. the 1981 Council of Europe Convention No. 108 and the 1980 Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines) and at a national level (e.g. the UK's Data Protection Act of 1984 and France's 1978 Act regarding informatics, files and liberties).

There was little harmonisation between these rules at an EU level. Some Member States applied strict limitations and procedures, whereas other Member States had no rules at all. This diversity constituted a barrier to the development of the internal market (the "first pillar"), and it was in this context that the Directive was created: as an internal market instrument designed to improve cross-border trade by harmonising data protection legislation.

[16] The distinction between the right to privacy in general and the protection of personal data can be seen clearly in more recent texts, such as the 2000 Charter of Fundamental Rights of the European Union, which includes separate provisions related to the protection of personal life (Article 7) and personal data (Article 8).

One of the crucial characteristics of the Directive is that it is tied to the concept of personal data, and not to a notion of privacy. Indeed, the provisions of the Directive can apply to acts of data processing which are not considered to be privacy sensitive in their own right. The Directive, therefore, serves a number of purposes, privacy protection being only one. Its rules fulfil a range of functions in practice, including encouraging freedom of expression, preventing discrimination and improving efficiency.

The influence of the Directive on data processing practices is undeniable: its principles have set the standard for the legal definition of personal data, regulatory responses to the use of personal data and other 'innovations in data protection policy'.[17] These include clarifying the scope of data protection rules, defining rights for data subjects, establishing the provisions regarding sensitive personal data and establishing supervisory authorities and transnational oversight arrangements in the form of the EU level Article 29 Working Party.

However, it is also important to realise that the Directive was written at a time when data processing involved filing systems and computer mainframes. The risks related to such a model could easily be managed by defining obligations and procedures linked to each role. Its main objective was to harmonise existing regulations to safeguard the data subject's right to informational privacy and to create a common European market for the free movement of personal data, not to create a legal framework that could cope with future data processing and privacy challenges.

The world has now moved on to a networked society where personal data is continuously collected, enriched, amended, exchanged and reused. It is clear that this new social environment needs well-adjusted data protection regulations to address the far greater risks of abuse. This leads to the question: is the current Directive, with its roots in a largely static and less globalised environment, still sufficiently flexible to handle the challenges of today?

1.2 The Directive as the main regulatory means of protecting data privacy for European citizens

The Directive comprises 34 Articles and its provisions include data quality, special categories of processing, the rights of data subjects, confidentiality, security, liability and sanctions, codes of conduct and supervisory authorities. It shares a number of basic concepts with other regulatory texts, such as the 1980 OECD Privacy Guidelines and the more recent Asia Pacific Economic Forum (APEC) Privacy Framework, as shown in Table 1.

[17] Bennett C.J. and Raab, C. *The Governance of Privacy: policy instruments in a global perspective*; 2nd Edition, MIT Press, London 2006 p 97

Table 1 Common privacy goals and principles

Goal	OECD Guidelines	APEC Privacy framework	Relevant article in the Directive
Legitimacy	Collection limitation principle	Preventing harm principle and collection limitation principle	Article 7: criteria for legitimacy
Purpose restriction (which implies data quality, purpose specification and proportionality)	Data quality principle, purpose specification principle and use limitation principle	Uses of personal Information principle, and integrity of personal information	Art 6: purpose and use restrictions, and quality/accuracy requirements (1)
Security and confidentiality	Security safeguards principle	Security safeguards principle	Art 16-17: Confidentiality and security of processing
Transparency	Openness principle	Notice principle	Art 10 & Art 11: the right to information regarding essential aspects of the data processing
Data subject participation	Individual participation principle	Choice principle; Access and correction principle	Art 12: right to access, which is sometimes coupled with the right to correct or delete the data
Accountability	Accountability principle	Accountability principle	Art. 22-23: rules on remedies and liability

(1) Personal data of an insufficient quality will inevitably be unsuitable for the purposes intended by the data controller; therefore data quality is an implied condition of the purpose restriction.

Source: RAND Europe & time.lex

While the Directive was not conceptually innovative, it has had a very powerful impact in the EU and can be credited with creating a binding and harmonised framework for data protection principles in all Member States.

However, data protection in Europe is not solely dependent on state-initiated regulation. Self-regulatory approaches are increasingly common, and include sector specific codes of conduct at national and international levels, the conclusion of contracts implementing binding Model Clauses or Binding Corporate Rules (BCRs) to cover the exchange of personal data with a party outside of the European Union,[18] and identity management to deal with challenges such as data ownership, data stewardship and data broking at a non-regulatory level. The Directive acknowledges and encourages these practices.

[18] See e.g. Working Party document WP 108, « *Working Document establishing a model checklist application for approval of Binding Corporate Rules",* adopted on 14 April 2005; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

1.2.1 Technical and organisational measures to protect personal data

While the Directive emphasises a regulatory approach, it provides indirect support for privacy protection through technology, most notably through Article 17.

Article 17 of the Directive requires data controllers to protect personal data against a variety of risks using the appropriate technical and organisational measures. Recital 46, which augments the meaning of Article 17, highlights that these measures should be incorporated into the design of the processing system and also the processing itself, so security cannot simply be added on to data systems, but must be built in; a principle that is now referred to as "privacy-by-design".

The European Commission reaffirmed its interest in so-called Privacy Enhancing Technologies (PETs) with its Communication of 2 May 2007,[19] which identifies and stresses the benefits of PETs, and lays down the Commission's objectives in this field.[20]

1.2.2 Role of the stakeholders: self- and co-regulatory approaches

Article 27 of the Directive encourages self- and co-regulatory approaches to data protection through codes of conduct. The popularity of codes of conduct varies from country to country.

At the national level, codes of conduct (typically sector-specific) are validated by national supervisory authorities. At the European level, codes can be validated by the Article 29 Working Party. Only two organisations have achieved European level validation so far: the International Air Transportation Association (IATA) and the Federation of European Direct and Interactive Marketing (FEDMA).

A secondary form of self-regulation can be found in the use of trust labels or privacy certifications, issued by independent bodies after assessing compliance with relevant data protection rules. While not referenced in the Directive, this method is sometimes used to establish trust with data subjects. Such schemes have not yet seen large scale take-up at the European level.

Co-regulation is occasionally applied in cross-border data transfers. The Safe Harbor Principles govern the export of personal data to self-certified organisations in the United States. A reported lack of official complaints suggests that this is a successful application of co-regulation.[21] The increasing interest in BCRs – albeit with limited impact in practice, for reasons that will be further explored below - is another example of the potential benefits of these approaches.

Irrespective of these examples, it is clear that self- and co-regulation have not taken on a key role in European data protection practices, despite the emphasis given to them in the

---

[19] *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs);* see also http://ec.europa.eu/idabc/servlets/Doc?id=28587

[20] For a practical scenario-based approach to PET enhanced electronic identification, see the 2007 *PRIME White Paper on Privacy-enhancing Identity Management*, 27 June 2007, R. Leenes ; https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V2.pdf

[21] While no official numbers are published, during interviews with a member of the US Mission to the EU, it was noted that complaints were quite rare, both from US and European citizens.

2003 Inter-Institutional Agreement on Better Lawmaking.[22] The low uptake is possibly due to a perception that they are "an enhancement rather than a substitute means of making data protection legislative requirements more effective and legitimate".[23] This is unfortunate given the relative success of self- and co-regulatory initiatives in the United States, the United Kingdom and the Netherlands.[24]

For self- or co-regulation to be effective, transparency, accountability, prevention of information asymmetry, aligning the interests of the self or co-regulatory institutions with those of the public, supervision, monitoring (by the government and stakeholders), and enforcement are all necessary.[25]

1.3 Perceptions of the Directive across Europe

Given this encompassing approach to data protection in the Directive, it is interesting to evaluate its perception, both by data subjects and by data controllers. The February 2008 Eurobarometer reports examining both perspectives[26] provide some interesting insights in this respect.

Broadly speaking, European citizens are conscious of privacy risks involved in the processing of their personal data, yet believe that the level of protection in their own countries may be inadequate, even under the Data Protection Directive.[27] However, mechanisms to improve these levels of protection such as the use of PETs or the intervention of data protection authorities were not well known, or at least not commonly drawn upon.

The perception from data controllers[28] is thus somewhat different from that of data subjects: they generally consider themselves to be fairly familiar with data protection regulations and consider the level of protection to be 'medium'. Faith in a regulatory approach to dealing with the increasing amount of personal information being exchanged

---

[22] *Inter-Institutional Agreement on "Better Lawmaking"* concluded between the EU Parliament, the EU Council of Ministers and the EU Commission of December 16, 2003 (2003/C321/01).

[23] WIK-Consult and RAND Europe: *Comparison of Privacy and Trust Policies in the Area of Electronic Communications - Final Report*, European Commission 2007 p. 10; see http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_20_07_07_pdf.pdf

[24] ibid p10. See also: *Implementing the Children's Online Privacy Protection Act – A Report to Congress* (Fed. Trade Commission, Feb. 2007), www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf

[25] Cave, J., Marsden, C. and Simmons S,; *Options for and Effectiveness of Internet Self- and Co-Regulation* TR-566-EC; RAND Santa Monica 2008 available at: http://www.rand.org/pubs/technical_reports/TR566/

[26] See the Eurobarometer; *Flash Eurobarometer Reports on Data Protection in the European Union: FL226 Data controllers' perceptions and FL225 Citizens' perceptions*, both available at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

[27] Eurobarometer; *Flash Eurobarometer Report on Data Protection in the European Union: Citizens' perceptions*, FL225; February 2008 available at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

[28] Eurobarometer; *Flash Eurobarometer Reports on Data Protection in the European Union: Data controllers' perceptions,* FL226; February 2008 available at: http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

was limited to about half of the respondents, which might explain why roughly the same amount of respondents indicated their use of PETs.

Complaints from data subjects were reported to be very rare, despite the aforementioned prevalence of doubts among two thirds of data subjects that their personal data was being handled appropriately. This could be indicative of either a lack of transparency (i.e. data subjects being unable to determine the relevant data processing practices) or a lack of confidence in the truthfulness of the disclosed information (i.e. data subjects not confiding in the information which the data controllers provide).

CHAPTER 2 The evolving context

2.1 Privacy in today's environment

This study comes at a high profile time for privacy and data protection. News media reports of breaches and misuse of personal data are a common, almost daily occurrence. In 2008 the UK Information Commissioner reported that there had been 277 cases of non-compliance involving personal information reported since 2007[29], with a significant quantity appearing from the public sector. In France, the CNIL fined Tyco Healthcare France EUR 30,000 in early 2007.[30] In Germany, Deutsche Telekom was found guilty of a breach of the German Federal Data Protection Act following the behaviour of corporate security staff in mining customer billing records.[31]

2.1.1 Economic drivers affecting privacy

Personal data can be described as the lifeblood or basic currency[32] of the information economy, being arguably a key asset, a central organising principle[33] and a critical enabler for business competitiveness in today's world. A number of studies describe the link between micro-economics, the use of personal data and the increase in contribution to Gross Domestic Product (GDP), national competitiveness and economic growth.[34] Using

[29] *ICO Data Breaches Count Soars to 277 with Most in Public Sector Despite HMRC* Computer Weekly available at: http://www.computerweekly.com/Articles/2008/10/29/232970/ico-data-breaches-count-soars-to-277-with-most-in-public-sector-despite-hmrc.htm 29th October 2008

[30] *Tyco France breaks employee data rules* The Register available at: http://www.theregister.co.uk/2007/05/29/tyco_breaks_france_employee_data_rules/; 29th May 2007

[31] *Deutsche Telekom Suspected of Breaches* Deutsche Welle http://www.dw-world.de/dw/article/0,2144,3357090,00.html; 24th May 2008

[32] The "currency of the Internet economy", as stated by Angel Gurría in the closing remarks to the 2008 *OECD Ministerial Meeting on the Future of the Internet Economy;* see http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html

[33] Identity has been termed the single organising principle in a wide variety of applications see for example *Information Assurance Advisory Council Initiative into Identity Assurance* 2006 available at http://www.iaac.org.uk/Default.aspx?tabid=105

[34] See generally Alessandro Acquisti's *The Economics of Privacy – Resources on Financial Privacy, economics, anonymity*, available at: www.heinz.cmu.edu/~acquisti/economics-privacy.htm and in particular Acquisti, A. *Privacy in Electronic Commerce and the Economics of Immediate Gratification.* Proceedings of ACM Electronic Commerce Conference (EC 04). New York, NY: ACM Press, 21-29, 2004.

personal data can lead to efficiency gains in existing marketplaces because organisations understand their customers' preferences better, and may create markets for wholly new services and companies.[35] Small, micro and medium sized-businesses can take advantage of personal data to reach a small or highly defined customer base.

The beneficial link between economic uses of personal information and macro-economic factors is not assured, however. Some companies may profit more than others from the use of such information, while excessive use can have a counterproductive effect, leading to trust being undermined.

Understanding how the private sector uses personal information can reveal how policies and regulations to protect privacy can be properly tailored to protect consumer rights without creating insurmountable or disproportionate barriers to business. For example, small and micro-businesses may find certain bureaucratic procedures burdensome and the various ways in which personal data may be used may require specific measures to provide for transparency and accountability.

Key economic drivers are the requirement for increased use of personal data which permits private and public sector benefits, which has an impact at the macro-economic level. These key economic drivers may be summarised as:

- Personal data helps companies efficiency gains (extracting more commercial value or profit from existing customers via better tailoring of products and services to the market) or enabling cost cutting in the private and/or public sector by eliminating inefficiencies but also
- innovation (providing new products and services based on understanding customers through the interrogation/re-use of their personal data);

However, there are other important economically driven factors which include:

- the increasing complexity of organisations, with outsourcing across multiple borders, partnering, off-shoring and complex relationships between those collecting and using personal data
- globalisation and the constant drive for competitiveness mean that personal data is moved where it is most efficient and effective for the organisation, highlighting uncertainty over whether rules that apply at the point of collection may still do so where this data is stored.

2.1.2 Societal drivers affecting privacy

Personal data can be used to benefit society as a whole. The public sector increasingly uses personal data processing to improve public services such as tax administration and social security provision. Managing personal data is seen as key to linking different government services, with the aim of providing a better 'service' to the citizen.[36] These might be

[35] Odlyzko, A. *Privacy, Economics and Price Discrimination on the Internet* Extended Abstract 2003 available at http://www.dtc.umn.edu/~odlyzko

[36] Deprest, J; *Secure e-environment: a key to realising a digital Europe* presentation given at SecurEgov working Conference, Brussels, 15th November 2007

facilitated by 'one stop shops' which pull together personal data from a variety of sources to facilitate easier access for the citizen. A good example of the way in which governments are looking to tailor services to the citizen include the UK's Transformational Government initiative.[37] Personal data is also being increasingly used in healthcare (particularly research and large-scale epidemiological studies) and socio-economic research[38].

The use of personal information to combat organised crime, identity fraud, illegal immigration and terrorism, for instance through the Data Retention Directive,[39] has also accelerated in response to recent geopolitical events.[40] Information is often sourced from databases compiled by private actors or by governments for other purposes, which has given rise to concerns about civil liberties, not least because the lines between stewardship and responsibility for personal data can become blurred when the private sector is made an agent of the state. Recent examples of this include the European–US debate over obtaining Passenger Name Record (PNR) data from airlines and details of financial transfers via the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[41]

The convergence of private services and public security can lead to diminished trust and increased risk of privacy threats, as personal data may be shared with neither little effective accountability nor any real clarity as to the recipients or goals of the data transfers.

There is extensive policy debate around 'finding the right balance between security and privacy',[42] which often minimises the fundamental role of human rights and the fact that, in a democratic society, measures that are harmful to an individual's privacy may only be taken when absolutely necessary.[43] Such measures may have unintended consequences. This is an issue which is handled very differently throughout Europe, with some countries focusing on data sharing between administrations to decrease redundancy and eliminate the risk of inconsistencies, while others adopt a sector specific approach to reducing privacy

---

[37] Walport, M. and Thomas, R., *Data Sharing Review* HMSO, London 2008

[38] E.g. see *2008 Annual Report* of the Commission Nationale de l'Informatique et des Liberties; Ch 1 Measuring Diversity: Ten Recommendations; Commission Nationale de l'Informatique et des Liberties, Paris 2008

[39] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

[40] E.g. see Crossman, G., et al *Overlooked: Surveillance and personal privacy in Modern Britain* Liberty; The Nuffield Foundation October 2007

[41] Reply from European Union to United States Treasury Department — SWIFT/Terrorist Finance Tracking Programme available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_166/c_16620070720en00260026.pdf

[42] Potoglou, P., Robinson, N. Kim C.W. et al.; *Quantifying individuals trade-offs between privacy, liberty and security: The case of rail travel in the UK.* International Choice Modelling Conference 2009, March 2009 (forthcoming)

[43] See for example; Gordon Brown *42 day detention: a fair solution* The Times Monday June 2008 and Blick, A, & Weir, S *The Rules of the Game: The Governments counter-terrorism laws and strategy*: A Democratic Audit Scoping Report for the Joseph Rowntree Reform Trust November 2005

risks.[44] In that respect, the Directive's exclusive applicability to 'first pillar' Internal Market issues means that its harmonising effect is similarly limited in scope.

The personal data agenda has become even more acute with recent e-Government initiatives, both national and Europe-wide.[45] Data sharing and biometrics are increasingly regarded as valid tools for combating serious crime and international terrorism, and the creation of extensive databases of fingerprints is planned for the near future, in spite of the privacy objections raised by civil society groups, data protection commissioners and supervisory authorities.[46] Identity cards for the general public containing electronic fingerprints are already being rolled out in some countries, with several more planning to deploy such systems.

Relevant societal drivers can be thus summarised as:

- Changing requirements of society in regard to social security, healthcare, national security and law enforcement resulting in the state increasingly turning to the use of personal data to deliver societal 'goods' deemed beneficial and acceptable as a privacy intrusion by either governments (unilaterally) or society at large
- The changing mentality of society in regard to privacy – evolving responsibility toward personal data; for example individuals willing to give up personal information for small gains such as by telling personal stories to become part of a trusted community of shared interests, and sharing content increasingly via user-friendly and accessible platforms such as YouTube and SNS.
- Evolving perceptions on the integrity of the human body and what it means to be human – trends toward plastic surgery & body alterations are beginning to impinge upon considerations of personal space and privacy as an increasing familiarity and comfort with technology that blurs the distinction between the human and the artificial attests.[47] The accelerating growth of technological enabled personal DNA analysis is another case in point.[48]

The individual can also contribute directly to how these factors play out because they use and manage the personal data of others. Examples include the large amounts of personal

[44] See the 2005 FIDIS Research Paper on ID-related Crime: *Towards a Common Ground for Interdisciplinary Research*; http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf

[45] See for example the European Commission's Interchange of Data Between Administrations, Citizens and Consumers programme at http://ec.europa.eu/idabc/

[46] Hustinx, P., *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection* European Data Protection Supervisor 10th November 2008

[47] See generally Voort, M vd and Ligtvoet, A.; *Towards and RFID policy for Europe: Workshop Report* http://www.rfidconsultation.eu/docs/ficheiros/RFID_Workshop_Reports_Final.pdf

[48] For example see *23andme – How It Works* https://www.23andme.com/howitworks/

data stored on mobile phones, Personal Digital Assistants and similar devices and social networking sites.[49]

Finally, when examining the societal value of personal data, the fact that personal data protection has an inherent value to society in itself should not be overlooked. Exercising such freedoms as the freedom of speech, freedom of association and the freedom to practice religion in a meaningful way requires that the individual has a suitable personal sphere to develop his or her convictions and decide how to exercise these. Privacy rights thus can act as a vehicle to exercise other rights.[50] Privacy protection is therefore not only essential as a safeguard for personal wellbeing, but also to ensure the needed freedom and creativity that may benefit society as a whole. Thus, for the purposes of defining more or less stringent data protection rules, the debate cannot be posed purely in terms of trading personal freedom for societal benefit. Privacy and data protection should not be characterised as a zero sum gain where an individual gain means a societal loss or vice versa.

2.1.3 Technology

Technology facilitates transfer and management of personal information, whether economic or social, and whether with or without consent. Electronic storage and transmission of data, particularly via the Internet, has thrown the privacy principles described earlier into sharp relief.[51] Many commentators suggest that technology will continue to "outpace…the imagination of even the most clever law-makers."[52] Indeed, the OECD is undertaking an assessment of its 1980 Privacy Guidelines in light of changing technologies, markets and user behaviour.[53]

The socio-economic drivers discussed above are enabled by a range of technological developments, such as ever faster and more efficient methods of data mining, and new ways of storing vast quantities of digital information on small and transportable devices.[54] Other technological advances that have an acute impact upon privacy include:

- *Ubiquitous personal communications devices* – camera / video enabled mobile phones are now used as media players, games consoles, location aware devices and interfaces to payment systems.[55] Their memory capacity is growing, and

[49] ENISA Position Paper: *Security Issues and Recommendations for Online Social Networks*; http://enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[50] Feinberg, J. *Freedom and Fulfilment: Philosophical Essays;* Princeton University Press 1994 p248

[51] E.g. see generally The Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, March 2007 available at: http://www.raeng.org.uk/policy/reports/default.htm

[52] The Hon. Justice Kirby M., *Four Parables and a reflection on Regulating the Net* 2008 available at: http://www.hcourt.gov.au/speeches/kirbyj/kirbyj_21feb08.pdf

[53] See, OECD, "*The Seoul Declaration for the Future of the Internet Economy*" (2008), available at: http://www.oecd.org/dataoecd/49/28/40839436.pdf

[54] Hustinx, P., *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive* Opinions of the European Data Protection Supervisor Official Journal of the European Union C 255 27th October 2007 p 2

[55] Miguel Helft and John Markoff 2007, "Google jumps into wireless world – It leads a drive to turn mobile phones into mobile computers", *International Herald Tribune*, 6 November.

individuals are increasingly storing a great deal of personal information on their mobile phones. Individuals can also become publishers permitting audio-visual recording of personal data to be collected and transferred to the internet for limitless onward transfer and persistent storage. The private sector is keen to use this information to better target marketing activities, and the public sector could use the data to deploy e-Government applications or achieve security and crime fighting objectives.

- *The Internet of Things and Services*[56] Communications networks and changes to the core architecture of the Internet and its protocols (e.g. Internet Protocol version 6, IPv6) will permit many more physical objects to have an Internet address, paving the way for a wide range of devices to be connected, such as vehicles, white goods and clothing. Combining these technologies with Radio Frequency Identification (RFID) could affect privacy in many ways, both good and bad.

- *Web 2.0* Examples of Web 2.0 include data mash-ups, where information is pooled from several distinct sources to provide a new service to the user, SNS, and blogging, podcasting, and life-casting.[57] Web 2.0 technologies can also enable business activities such as behavioural advertising, which targets customers based on an in-depth understanding of their online browsing habits. Other commercial aspects of Web 2.0 include web-based Service Orientated Architectures (SoA), where standard protocols that allow separate services to interact are established, and electronic payment systems, such as PayPal, which act as a trusted third party for payment.

- *Electronic Identity Systems (eIDs)* are becoming increasingly attractive to both the private and public sectors: mostly using smart card or biometrics. In the private sector, eIDs are used to control access to workplaces, travel and payment as well as for identification and authentication. In the public sector, eID technology is being used in identity management applications that enable access to government services, provide efficiency gains by reducing the administrative burden for government back-office functions, and support the fight against organised crime and terrorism.

- *Virtualisation technologies* enable individuals to share the same IT resources irrespective of their geographic or technological situation.[58] Organisations can use virtualisation technology to achieve significant economies of scale by moving information (frequently personal data) across the globe between modular and reconfigurable data centres,[59] often managed remotely. Virtualisation thus makes

---

[56] *Internet of Things 2008* International Conference for Industry and Academia, March 26-28 2008, Zurich.

[57] Hi-Tech ways to stay in touch 7th November 2007 *BBC News* available at http://news.bbc.co.uk/2/hi/technology/7082566.stm

[58] Whatis.com Definition *Virtualisation: A Whatis.com definition* http://searchservervirtualization.techtarget.com/sDefinition/0,,sid94_gci499539,00.html

[59] e.g. Google's use of a cloud computing model in the delivery of its Gmail email service

the repeated replication, cost-free transfer and immortality of personal information a reality.

2.1.4 Challenges for privacy protection

Circumstances have changed fundamentally since the European Data Protection Directive was created. The fluidity of personal data collections has increased as the scope, goals and ownership of such data continuously evolve. European citizens are becoming increasingly involved in managing their own data (e.g. by choosing permitted recipients or allowing preferred applications to re-use their data) through social networks, an interesting avenue of control that was not envisaged by the Directive. Thus the Directive faces a number of challenges if it is to remain valid in a fast-changing world.

- *Multitude of perceptions of privacy*. The perception of privacy as a fundamental right changes depending on those concerned and the context in which this right is being exercised. For example, privacy in economic transactions is frequently treated as a resource to be traded for economic benefits. In interactions with the public sector, when this information might be used to make judgements affecting liberty or freedom, privacy is more likely to be interpreted in terms of fundamental human rights.
- *Risk assessment*. The risk of personal information being misused, either intentionally or accidentally, cannot be accurately perceived in advance[60] although it is possible to determine general typologies. The perception of the severity and impact of such risks is also highly dependent upon cultural and historical contexts.
- *The rights of the individual in relation to the rights of society*. While individuals may trade their personal data for economic benefit, they may also have to waive their right to privacy in the interests of broader societal benefits, for instance to address national security threats. Under what circumstances can personal privacy become secondary to the needs of society considering the fundamental importance of privacy protection for the development of democratic societies as a whole?
- *Transparency*. Where and how personal information is stored and used is becoming increasingly opaque due to technological advances and increasing globalisation. The fact that personal information may become persistent and costs nothing or very little to transfer may affect the security and transparency with which such information is used.
- *Exercising choice*. Using personal information to achieve management efficiencies and deliver new services may affect the ability of individuals to exercise meaningful choice. If individuals cannot exercise choice because they are unwilling to submit personal information, then they may be damaged economically, excluded, disenfranchised or be exposed to other potential risks.

[60] 6, Perri; Whats in a frame? Social Organisation, Risk Perception and the sociology of knowledge; *Journal of Risk Research* Vol 8. no 2 pp 91 - 118

- *Assigning accountability*. It is extremely difficult to predict how public and private sector organisations might wish to use personal information in the future.[61] Accountability provisions must be flexible enough to be applied in different cases and suitable for the context in which personal data is used. This may mean that accountability measures for organisations that are sensitive to economic drivers might be different to those for the public sector or individuals, as accountability based on economic sanctions can be expected to be more effective in situations where the incentive for personal data processing was created by considerations of direct economic benefit.

2.1.5 Summary of the way that current arrangements face up to these challenges

As was noted above, the Directive's scope is very closely tied to the notion of personal data, which is defined in the Directive in fairly strict terms, based on the linkability to individual data subjects. Using this notion as a building block, specific roles are defined in addition to that of the data subject, including those of the data controller and data processor, which are linked to specific acts of data processing (i.e. a controller in one act of data processing may become a processor in the next). Rights and obligations are defined in relation to these roles, including specific processes (information obligations, notifications, adequacy findings, etc.) to ensure that general data protection principles are observed.

In the section below, we will examine how this approach stands up to the aforementioned challenges. Based on these challenges, it is clear that an effective legal framework needs to take into account the ease and scope with which personal data is continuously being used and re-used across multiple contexts, and on the enabling role that technology can play in this regard, both as a privacy enabler and as a privacy threat. In addition, national boundaries play even less of a role today than they did when the Directive was originally created, which means that a well adjusted legal framework needs to function efficiently in an international context. Finally, in order to retain its credibility towards data controllers and data subjects alike, the legal framework needs to ensure that the obligations it imposes are proportionate to the risks involved in personal data processing, and that the data subjects have the right and possibility to effective legal recourse in case of incidents.

Generally, it is clear that there is a need for a flexible framework that allows data controllers to create and offer products and services at an international scale, while ensuring that data subjects retain their right to efficient data protection through effective enforcement and accountability mechanisms. This requires a legal framework that is sufficiently focused on real data protection impact and practical outcomes. Below, we will assess how the Directive measures up to these needs.

[61] Lace, S. (ed) *The Glass Consumer: Life in a Surveillance Society* National Consumer Council London 2006

CHAPTER 3 How does the Directive stand up to current challenges?

3.1 Introduction

In order to evaluate whether the Directive is meeting its goals, we must examine how the Directive stands up to the challenges identified in Chapter 2. To do so, we must identify and analyse the main strengths and weaknesses of the Directive, keeping into account both the provisions of the Directive and their impact and effectiveness in practice. In the sections above, it was already noted that the Directive aimed to improve the individual's right to privacy with respect to the processing of personal data and to enable the free exchange of personal data between the Member States (Article 1 of the Directive). Below, we will examine if these objectives have been reached, and to what extent any weaknesses can be attributed to problems in the Directive itself.

In addition, it is necessary to consider the broader international context. One of the main challenges identified above is that personal data is increasingly processed in an international context. This implies that the regulatory framework adopted by the Member States must offer effective and tangible protections at the non-European level as well. As we shall see below, some characteristics of the Directive's approach to the protection of personal data can be considered typically European, and are not necessarily considered to be equally crucial in regulatory instruments originating outside of the EU. Apart from the Directive's scope being limited to internal market issues, these European elements include most notably:

- An approach that focuses not only on principles to be observed or goals to be achieved, but also on the procedures to be followed to realise the desired goals. This is one of the main differences between the Directive and e.g. the OECD Principles or the APEC Privacy Framework, where the latter generally take a principles based approach that focuses more on effect rather than process. For instance, while all three texts provide for data collection and data use principles, only the Directive approaches this issue as a ban against the processing of personal data in general unless one of six conditions is met.
- The strict approach towards transferring personal data to third countries. The OECD Principles emphasise the principle of free flow of data between OECD Member countries. The Directive embraces a similar free flow principle for

Member States (article 1.2 of the Directive), but places a much stronger emphasis on restricting data exports to other countries unless specific and strict requirements are met. This is an element that could contribute to a perception of paternalism, as European data protection regulations are presented as a yardstick for the adequacy of similar frameworks abroad.

- The importance of independent supervision. Supervisory authorities in all Member States have broad competence to investigate data protection issues, provide guidance and engage in legal proceedings. They must be also consulted when regulations with a potential data protection impact are drafted. This emphasis on independent supervision is a crucial characteristic for the European approach to data protection.
- The definition of specific classes of sensitive data in Article 8 of the Directive and the introduction of more stringent rules for such classes. While other non-European frameworks also require data controllers to take the sensitivity of personal data into account, they do not explicitly enumerate these categories of data nor provide specific additional rules and restrictions.

In the sections below, we will examine the strengths and weaknesses of the Directive, taking into account the goals and challenges.

3.2 Main Strengths

Table 2 summarises the main strengths of the Directive and national implementations based on the literature review and interviews conducted for this study.

Table 2: Summary of Main Strengths

Strength	Evidence
Serves as reference model for good practice	Legislation that permits practical exercise of fundamental rights derived from ECHR, and considered a leading international model. Other privacy legislations adopt elements from the Directive e.g. Hong Kong, Canada, parts of Latin America
Harmonises data protection principles and to a certain extent enables an internal market for personal data	Implementation of legal rules across Europe for personal data processing that have greater compatibility than prior to the Directive's introduction
Flexible due to a principles-based framework	The Directive defines principles, without going into details for specific sectors/contexts. The exception to this rule is direct marketing
Technology neutral	No reference to specific technologies Security measures not specified Concept of personal data broad enough to be technologically neutral
Improves general awareness of privacy issues	Establishment and increasing numbers of privacy policies, privacy officers, etc. Consumer awareness regarding privacy

Source: RAND Europe & time-lex

3.2.1 The Directive as a reference model for good practice

One of the most frequently quoted positive aspects of the Directive was the impact it has had in structuring and organising the debate surrounding data protection. While the OECD Guidelines were very influential in shaping this debate, the Directive can be credited with formulating legally binding rules that have become effective law across the Member States, following in the footsteps of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

As a result, the Directive is internationally respected, and its principles are often held up as a standard for good data protection practices even in contexts where it does not apply directly. Indeed, the APEC Privacy framework is one example where the provisions of the Directive have had a clear influence.

A number of other jurisdictions are considering legislative reform based on the Directive. These include Hong Kong and several jurisdictions in Latin America, including Chile and Ecuador. The Directive was illustrative in inspiring Canada to develop its own Personal Information Protection and Electronic Documents Act (PIPEDA). Other examples of the Directive's influence can be found in the way that it has inspired the creation and

recognition of the importance of supervisory authorities. The OECD refers to such bodies as Privacy Enforcement Authorities – reflecting a slightly different perspective of their role, emphasising their enabling role as privacy enforcers especially in a cross border context – and has recently developed a framework to facilitate co-operation among them.[62].

The goals and principles adopted by the Directive, following the earlier examples of the OECD Guidelines and the Council of Europe Convention No. 108, have become an integral part of the European privacy debate. Whenever privacy issues are discussed in relation to data processing in whatever sphere, objections can often be traced back to the principles expressed by the Directive. This can be seen for example in debates around how long telecommunications companies should keep data under the Data Retention Directive.[63] The proportionality principle plays a central role here: under the European Convention for the Protection of Human Rights and Fundamental Freedoms, any derogation of the right to privacy is only permissible subject to a number of conditions, including its necessity in a democratic society (Article 8 of the Convention), which implies that such derogations should be kept to the strict minimum required to achieve the envisaged legitimate objective. This principle is embodied in the proportionality requirements of the Directive, and should equally be respected by the Data Retention Directive.

3.2.2 Harmonising data protection principles and enabling an internal market for personal data

One of the key goals of the Directive was to improve the harmonisation of data protection rules across Member States, in order to ensure the right to privacy with respect to the processing of personal data and to permit the free flow of personal data between Member States (Article 1 of the Directive). The aim was to create a sufficiently harmonised European legal framework so that data controllers managed personal data in accordance with the same principles in any Member State, and data subjects would have clear rights regardless of where they or the data controller were located.

The Directive has ensured that broadly comparable legal rules for crucial aspects of personal data processing are in place throughout the EU. These include the concept of personal data, requirements for legitimacy, data quality and security, data subjects' rights and the possibility of enforcing these rules, as described by Korff.[64]

---

[62] OECD, "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy" (2007) available at: www.oecd.org/sti/privacycooperation.

[63] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

[64] Korff, D. *EC Study on the Implementation of the Data Protection Directive* - comparative summary of national laws; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf

3.2.3 Flexibility due to a principles-based framework

Many of the Directive's obligations remain relatively high level. The framework approach based on principles allows Member States to implement the necessary measures while taking into account local traditions and sensitivities, and the needs of specific sectors.

This flexibility can be seen in the case of direct marketing. It was observed during interviews with representatives from the direct marketing sector that Northern European countries are more open to direct marketing and legislate accordingly, while Southern European countries have more formal and stricter sets of rules. While the Directive itself contains certain restrictions with regard to personal data processing in the context of direct marketing – most notably the data subject's right to object to such data processing as foreseen in Article 14(b) – other aspects of direct marketing continue to diverge, and this national divergence (as a reflection of differing societal attitudes) was, perhaps surprisingly, characterised during these interviews as acceptable and even beneficial.

3.2.4 Technology neutral

To a large extent[65], the Directive does not concern itself with the way its provisions should be applied in specific sectors (e.g. financial services) or in the context of new technologies (e.g. RFID).

The definition of personal data has been left deliberately abstract so that it can be applied in a number of technological contexts. The definition relies on considerations of 'content', 'purpose' and 'result', and can thus be applied to biometric data, behavioural data or characteristics that may be assigned by a data controller (e.g. passport number). The Opinions of the Article 29 Working Party on RFID and on the concept of personal data, and the responses to the 2002 Implementation Review concerning audio-visual information, attest to this flexibility.

The legal framework is therefore not limited to a specific societal and technological context, and so national data protection authorities can clarify how the Directive's provisions should be applied in each context, if needed. The Article 29 Working Party thus provides European level interpretations when required.

3.2.5 Fostering a greater general awareness of privacy issues

The inclusion of data protection considerations in bilateral trade negotiations between the EU and other countries (e.g. South Africa, Mexico and Thailand) indicates that awareness of data protection is improving. Agreements currently being negotiated between the European Commission and the Caribbean Community (CARICOM) and Central Africa are being amended to point to the Directive instead of OECD and UN principles.

The Directive raises awareness by stating high level goals and the way in which these goals should be achieved, and by promoting data protection tools that include notification, model contracts, standard contractual clauses, privacy policies and the appointment of Data Protection Officers. Notification, for instance, promotes the transparency goal by requiring that Data Controllers provide information about the data processing methods

[65] The reference to direct marketing in article 14 (b) of the Directive is a noteworthy exception.

they intend to use and obliging them to make sure their data protection practices comply with the Directive.

The transparency provisions have also helped individuals become more aware of privacy issues, especially regarding notice, consent, and choice. Interest and awareness[66] is demonstrated by responses from customers when notified about changes in privacy practices, and direct communications about uses of their personal data.

[66] See generally *Eurobarometer Report on Data Protection in the European Union: Citizens' perceptions*, published at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

3.3 Main Weaknesses

Table 3 summarises the main weaknesses of the Directive and national implementations based on the interviews conducted for this study. Problems with national implementations can be indicative of insufficient harmonisation with the provisions of the Directive; for instance, if implementation functions well in some countries but not in others, this may indicate that the Directive leaves too much margin for interpretation.

Table 3: Summary of Main Weaknesses

Weakness	Evidence
The link between the concept of personal data and real risks is unclear	The application scope of the Directive depends too strongly on whether or not the data processed can be defined as "personal" data. It is all or nothing: there is no room for "more or less personal" data (and accordingly "more or less protection"). Special categories of personal data processing are explicitly defined; but financial information and location data are not classified as sensitive. Strict application of the Directive's concepts sometimes leads to unpredictable or counterintuitive results.
Measures aimed at providing transparency of data processing through better information and notification are inconsistent and ineffective	Privacy policies not read in practice, as they are aimed at consumers yet written by/for lawyers Privacy policies do not play a role as a market differentiator Unclear purpose of notification Variety of 20 different notification processes, variety of exemption rules Uneven implementation of the process of registration
The rules on data export and transfer to third countries are outmoded	Definition of 'third countries' is perceived as outmoded in the light of globalisation Adequacy of countries is not relevant to business realities or to data protection Regulation in some other countries is stronger than the EU, but still not recognised as adequate
The tools providing for transfer of data to third countries are cumbersome	Length of time and effort required to get Standard Contractual Clauses, model contracts or Binding Corporate Rules approved is excessive Uneven practices of approval and authorisation; too little coordination between the Member States
The role of DPAs in accountability and enforcement is inconsistent	Unclear rationale for enforcement Uneven implementation of enforcement across Member States either for punishment or to affect behaviours Differing criteria for imposing sanctions
The definition of entities involved in processing and managing personal data is simplistic and static	Globalisation and increased re-use of personal data has outpaced the static definitions of controller and processor.

Source: RAND Europe & time.lex

3.3.1 The link between the concept of personal data and real privacy risks is unclear

The scope of the Directive has been criticised because the relationship between privacy protection and data protection is vague: not all acts of personal data processing as covered by the Directive have a clear or noticeable privacy impact, and we must ask if this is a weakness in its focus. Should the impact on privacy be a relevant criterion for determining the applicability of data protection rules?

The impact of the Directive is not defined in terms of situations with a privacy impact, but rather to acts of personal data processing. The Directive's approach is based strongly on a fundamental rights interpretation of data protection, where personal data is deemed inherently worthy of protection.

However, the notion of personal data is extremely broad and subject to much debate. Some argue that any data that could be linked to a specific individual should be considered as personal data. Under this absolute interpretation, Internet Protocol (IP) addresses are personal data, regardless of whether the entity processing them has a realistic possibility of linking them to a given individual. Freely chosen user names, even those that contain no semantic link to a user, and geographical information are also problematic. Data such as those in Google Streetview may come under the Directive if they include images of individuals.

Anonymity in large datasets is also complicated. Healthcare research is one area that uses large sets of anonymised clinical data for statistical analysis, data mining etc. However, regardless of how rigorously the data is de-personalised, legally speaking under this absolute interpretation it remains personal data if there is a possibility of linking the data to an individual, however remote, difficult or complex that may be.

A more relative interpretation of personal data was recently described in Opinion Nº 4/2007 of the Article 29 Working Party[67], which noted that, in order to find that data "relate" to an individual, either a "content" element, a "purpose" element or a "result" element should be present. This means that data is personal data when it contains information about a specific person (content), when it is used or likely to be used to determine the treatment of a specific person (purpose), or when it is likely to have an impact on a specific person (result). Thus, IP addresses, user names or maps might not always be classified as personal data, the context within which the data is processed must be examined to determine whether one of the three criteria have been met.

Determining what constitutes personal data becomes particularly acute in the context of mobile telecommunications, where a device with an IP address may easily be used by another entity. The problem is likely to get worse with IPv6, when IP addresses will become much more widely available and begin to be assigned to objects such as home appliances or cars.

While the relative interpretation is more flexible than the absolute one, the three criteria are still very broad. For instance, a website that uses IP addresses to determine the likely origin of a visitor for language customization purposes clearly uses information "to

[67] Art. 29 WP *Opinion Nº 4/2007 on the concept of personal data* (WP136 - 01248/07/EN); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

determine the treatment of a specific person" and "to have an impact on a specific person". Thus, data protection rules would apply, regardless of the apparent lack of privacy risk.

The Directive's rules on special categories of processing could also benefit from reconsideration. As it stands, the Directive acknowledges that certain types of personal data are more privacy sensitive and more likely to harm the data subject in cases of unauthorised processing. These include 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" (Article 8 paragraph 1 of the Directive). Based on this, more stringent conditions for the processing of such categories are imposed.

However, while potential harm (such as discrimination) should be considered when determining security measures, such generic categorizations are often difficult to apply in practice. For instance images often reveal racial origin, and names may be typical to certain ethnicities and/or religions. The 2002 Proposals for Amendment[68] suggested redefining the scope of this provision in terms of acts of data processing that include any kind of discriminatory practice, i.e. those that might affect a specific person.

In addition, the special categories contain some surprising omissions, for instance financial and location data. The interpretation of location data (e.g. which locations are visited, suggesting which shops are frequented, and which products and services are bought), may in the future permit the identification of the health, social, sexual or religious characteristics of the data subject. Location based services provided via mobile devices are already seen as a growth market. This is an example of one aspect (protection of special categories of data processing) where the Directive appears to have favoured a process oriented approach focused on linking specific obligations to formal criteria, rather than on an outcomes based approach that would consider the impact and the necessity of such obligations.

3.3.2 Measures aimed at providing transparency through better information and notification are inconsistent and ineffective

One of the goals of the Directive is to make data processing more transparent to data subjects. In order to achieve this goal, data controllers are required to provide certain information to the data subject, and in some cases to register a notification with the national data protection authority.

The information obligation is contained in Articles 10 and 11 of the Directive, which distinguish between situations where the data is directly (Article 10) or indirectly (Article 11) obtained from the data subject. In both cases, there is a list of information that must be provided to the data subject.

The main way of providing this information is via a privacy notices, privacy policies or consent notices. While there is no strict definition of these types of documents, notices can be considered to be accessible texts aiming to inform the average data subject; policies contain specific legal information delineating data subjects' rights and data controller's obligations; and consent notices are aimed at obtaining the data subject's informed (in

[68] The *2002 Proposals for Amendment of the Data Protection Directive (95/46/EC),* made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note, http://www.dca.gov.uk/ccpd/dpdamend.htm

principle) consent for certain data processing activities, e.g. by ticking a box. Ultimately, these texts should provide consumers with the information needed to exercise their rights, and become a factor in how they value offerings.

In principle, there is no problem with the information obligation as stated in the Directive. The lists of required information focus on the information that the data subject reasonably needs. However, the term "provide" used in the Directive seems to imply that active communication is necessary, rather than, for instance, making sure that the relevant information can be found easily on a website or elsewhere. This can be difficult to apply in practice, and depends on the degree of interaction between the controller and the data subject and how they communicate (e.g. through pop-ups, SMS messages etc.). Furthermore, by interpreting the transparency requirement as necessarily requiring an active communication, the Directive is no longer adapted to the social evolution seen in the last decade, where consumers have become more accustomed to finding relevant information themselves.

More importantly, while privacy policies are considered to be the main way of obtaining consent from a data subject in the online world, consumers feel very strongly that current mechanisms do not help them to understand their rights.[69] The evidence suggests that their use is predominantly targeted to meet any applicable legal transparency requirement, rather than serving a real transparency benefit towards the consumer. Privacy policies are written by lawyers, for lawyers, and appear to serve little useful purpose for the data subject due to their length, complexity and extensive use of legal terminology.

Privacy policies may also differ significantly from one Member State to another. In some countries, for example, each privacy policy must state the relevant applicable decree, whereas in others the relevant law does not need to be referenced. Due to the pressures of efficiency and speed, service providers may opt to draft one privacy policy that is compatible with the most stringent legislative requirements in the hopes that this will cover the requirements of other Member States. Interviewees also mentioned that legal requirements for consent in certain countries were so restrictive that companies were dissuaded from investing in those countries.

Recent comments from the Article 29 Working Party on improving the accessibility of privacy policies by making them easier to understand were regarded as somewhat naïve by those in the commercial sector, and contradictory. This is because some national laws require full descriptions of data processing activities, and it is very difficult to describe them in a form the consumer can understand.

In addition, privacy policies have hidden costs. A recent experimental economic study of US privacy policies illustrates the potential economic damage that would result were

---

[69] E.g. see Scribbins, K., *Privacy@net – an International Comparative Study of consumer privacy on the internet* Consumers International - Programme for Developed Economies and Economies in Transition; 2001 available at
http://www.consumersinternational.org/Templates/Internal.asp?NodeID=91787%20&int1stParentNodeID=89648&int2ndParentNodeID=89652&int3rdParentNodeID=89792&int4thParentNodeID=89708&int5thParentNodeID=89708&int6thParentNodeID=89708&int7thParentNodeID=89708&int8thParentNodeID=89708&strSubSite=1&strLHSMenu=89648

consumers to read each policy. The cost to the US national economy just for reading each privacy policy was estimated to be $365bn, based on the length of time it takes to read a privacy policy and the monetary value of that time.[70]

The end result is that privacy policies are not read. Companies have evidence indicating that few consumers access privacy policies. This does not necessarily demonstrate lack of interest – users notified about new privacy policies often ask questions. Surveys by Eurobarometer[71] and the social networking site Facebook[72] indicate that privacy awareness does exist, but that users do not view the privacy policy as a means of expressing their consent with its contents. An understanding that consent has already been implicitly given by accessing the service may help to explain this.

In that respect, the role and rights of the data subjects as currently formulated in the Directive could benefit from reconsideration. Consent is currently given an important role, both in the Directive as one of the possible criteria to legitimise data processing, and in practice through the use of privacy policies or data protection clauses in contracts. However, given that such clauses are not typically read in practice, it can be questioned whether the Directive's requirement of 'freely given specific and informed indication of his wishes' (Article 2 (h)) is often realised. In this respect, it is interesting to note the approach taken with regard to consumer protection, where Community regulations[73] have adopted rules to protect consumers against the effects of unfair standard terms in contracts concluded with professionals. In effect, this is a recognition that consumer consent with standard terms is often very relative, and that it should be possible to set unfair terms aside, even if the consumer originally consented to them. If this is the case, effective data protection is better served by ensuring that the data subject has access to efficient tools to enforce his rights than by overemphasising the legitimising capacity of consent on specific instances of data processing. This should not be taken to imply that privacy policies or similar texts have no beneficial impact. Indeed, they can be usefully referenced in case of incidents, either by the consumer to determine how these could be addressed, or by enforcement bodies as a tool to identify the restrictions that the data controller self-imposed through such texts. In this way, privacy policies and similar texts can be used as tools to facilitate enforcement (similar to the potential use of notifications to DPAs), which

---

[70] McDonald, A.M. and Cranor, L.F. *The Cost of Reading Privacy Policies* Preprint for Telecommunications Policy Research Conference November 2008

[71] See the Eurobarometer *Reports on Data Protection in the European Union:* Data controllers' perceptions and Citizens' perceptions, both published at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

[72] Thomson, M, presentation given at the *30th International Conference of Data Protection and Privacy Commissioners* "Protecting Privacy in a Borderless World" 15th – 17th October, Strasbourg 2008 (video of the presentation available at: http://www.privacyconference2008.org/index.php?page_id=194&video=video/081015_w03_w.wmv)

[73] See e.g. Council Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts (published in the Official Journal of the European Communities, No. L 95 of 21 April 1993, p. 95); and Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (published in the Official Journal of the European Communities, No. L 149 of 11 June 2005, p. 22);

seems to be a more realistic assessment of their benefit than presenting them as tools to improve transparency towards data subjects or to obtain informed consent.

In relation to the data subject's other rights, most notably the right to access personal data relating to him or herself, there is debate as to whether this has been efficiently enshrined in the Directive.[74] Specifically, it has been questioned whether the exercise of this right could be made subject to specific conditions, such as the ability of the data controller to reasonably locate the data (important in a non-electronic context and in an electronic decentralised or 'cloud' environment), and the obligation of the data subject himself to assist in locating the data when appropriate. However, in response to this, the European Commission has already noted in its First Implementation Report[75] that "[...] the possibility of asking for such assistance is already in conformity with the Directive in its present form. […] The Commission considers the interpretations and guidance provided by national supervisory authorities so far to be wholly reasonable." The European Commission thus rejected the need for clarifications to this right, arguing that the Directive already offered the Member States a reasonable flexibility. The problems reported by stakeholders thus seemed to relate more to a matter of implementation.

The notification obligation (Article 18 of the Directive) requires a data controller to notify the relevant national supervisory authority before carrying out specific acts of data processing. Exemptions and simplifications are allowed in a limited number of cases where the rights and freedoms of the data subject are unlikely to be adversely impacted. This obligation is intended to enhance transparency for data subjects, raise awareness for data controllers and give data protection authorities a useful monitoring tool in the form of registers.[76]

Such notification may have been suitable when processing personal data was a static, localised process, but now such processing has become widespread in many spheres, even in personal and domestic situations, and better avenues are available to ensure transparency.

The actual process of notification was seen as the most important weakness by many of those currently involved in the domain. It was seen as an example of poor harmonisation and a barrier to the internal market, since there were numerous different ways of notifying data processing, depending on the country.

Currently, each Member State has its own rules for notifications and exceptions, which results in very high costs and workloads for data controllers and DPAs alike, with no proportionate benefit corresponding to this diversity. In some countries, notification is based on what personal data is being processed by the organisation, whereas in others it is

---

[74] See e.g. the *2002 Proposals for Amendment of the Data Protection Directive (95/46/EC),* made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note, http://www.dca.gov.uk/ccpd/dpdamend.htm

[75] *European Commission's First Report (2003) on the transposition of the Data Protection Directive*, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT

[76] *Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive* (07.03.2007); see http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf

based on the systems being used to process the data. The amount of detail required varies, in Poland for example, every data processing system and the associated security measures must be described in each notification. The level at which notification is required also varies, ranging from none at all, to internal transfers, to transfer to third countries. This can have a crippling impact on the effectiveness of the obligation, as obligations which are perceived as excessive, unnecessary or ineffective are more likely to be ignored in practice.

One specific instance was identified where a separate license or permit is required for third country data transfer. It was indicated that, since it took so long to obtain such licenses, some organisations do not wait for them to be issued. If these transgressions were to be acted on, businesses could face significant economic damage.

The purpose of the notification process as a register was also questioned. In some countries, the notification process was perceived as an indirect form of taxation to fund the regulator, but this was not the case in other countries, which had different forms of funding, including governmental grants. However, in the latter case, it has to be ensured that such grants in conjunction with other control mechanisms cannot be seen as breaching the requirement of supervisory authorities to be independent.

Registers of data controllers were seen as only useful to lawyers conducting due diligence exercises. It was noted that consumers did not seem to be consulting the registers, either because they were unaware of them, or because they were unable to use the information in the registers to determine whether or not their own data was being processed.

There was a wide gap in the evidence between the number of notifications reported by the supervisory authorities and the likely number of data controllers in each country.

The Commission has expressed sympathy for the complexity of diverging implementations, but feels that it is up to Member States to simplify their own regulations.[77] Efforts to harmonize the existing diversity have not yet materialised to our knowledge,[78] despite requests to this effect.[79, 80]

---

[77] As noted in the 2003 First Implementation Report: "Many submissions argue for the need to simplify and approximate the requirements in Member States as regards the notification of processing operations by data controllers. The Commission shares this view, but recalls that the Directive already offers the Member States the possibility to provide for wide exemptions from notification in cases where low risk is involved or when the controller has appointed a data protection official. These exemptions allow for sufficient flexibility while not affecting the level of protection guaranteed. Regrettably, some Member States have not availed themselves of these possibilities. However, the Commission agrees that, in addition to wider use of the existent exemptions, some further simplification would be useful and should be possible without amending the existing Articles." Commission's First Report (2003) on the transposition of the Data Protection Directive

[78] 'The European Commission shares to a large extent the criticism expressed by data controllers during the review concerning the divergent content of notification obligations placed on data controllers. The Commission recommends a wider use of the exceptions and in particular of the possibility foreseen in Article 18(2) of the Directive, that is the appointment of a data protection officer which creates an exemption from notification requirements.' Report from the Commission – *First report on the implementation of the Data Protection Directive* (95/46/EC). COM/2003/0265 final.

[79] See e.g. the 2002 *Proposals for Amendment of the Data Protection Directive (95/46/EC),* made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note, http://www.dca.gov.uk/ccpd/dpdamend.htm

3.3.3 The rules on data export and transfer to external third countries are outmoded

One of the best known provisions of the Directive relates to the transfer of personal data to third countries. The Directive imposes restrictions on such data transfers to prevent personal data from being moved to countries where the data protection regime is less stringent.

Our interviewees felt that having specific rules for transfers to a third country was no longer appropriate in an era of globalisation. They believed that distinguishing between countries inside and outside the EU was unnecessary and counter-productive in the modern world. For multi-national organisations operating across boundaries but applying the same high standards of data protection across all geographical divisions, this mechanism made no sense and was seen as contrary to harmonisation and global trade.

Although the provision seeks to protect the data of European citizens, the sheer quantities of personal information transferred overseas may undermine this. It remains to be seen whether European citizens whose data is used and moved around by entities governed by legal frameworks outside the EU have the same level of protection.

The general rule presented by the Directive states that such transfers are only allowed if the third country ensures "an adequate level of protection", the adequacy rule. If this is not the case, certain alternative paths are available, such as the consent of the data subject, or the adoption of certain standard clauses or BCRs.

The adequacy rule found very little support among our interviewees. It was labelled as highly restrictive and polarizing, resulting in a mechanism where only countries that follow the Directive strictly are considered to have an adequate protection regime. De facto, the test being applied to third countries is not an adequacy test, but an equivalence (i.e. transposition) test.

The system for assessing third counties was considered ineffective and too limited. After 13 years, only 5 non-EU countries have been found to have adequate legal frameworks: Switzerland, Canada, Argentina, Guernsey, Jersey and the Isle of Man.[81] Current and emerging trade powers such as China, India, Brazil, Japan and Russia, are not included, and the US is only covered through the 'Safe Harbor' Privacy Principles (and to a lesser extent the transfer of PNR data to the Bureau of Customs and Border Protection). Interviewees considered that adequacy assessments as currently conducted were merely a review of paper and policy, rather than a serious investigation into how personal data is

[80] Such efforts are also supported to a certain degree by the Article 29 Working Party: "Data Protection authorities within the Article 29 Working Party agree on the need to streamlining the exemption system by inviting the Member States where some exemptions are not provided for to consider possible harmonisation attempts. It would be desirable that data controllers could benefit from the same catalogue of exceptions and simplification everywhere in the European Union." Working Party document WP 106 - *Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union*, adopted on 18 January 2005; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf

[81] DG Justice Freedom and Security ; *Decisions on Adequacy of Third Countries* available at : http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

actually protected in the candidate country, and occasionally questioned whether they currently constituted a credible test of data protection realities.

In addition, the adequacy rule was considered to be inappropriately focused. When determining whether the personal data of a specific subject is sufficiently protected in a third country, it is important to know that: (a) the data controller has taken sufficient measures to achieve this objective; and (b) the data controller can be held accountable for any incidents. The presence of an adequate legal framework that appears to match the provisions of the Directive in the third country does not address this problem fully. It was suggested by some interviewees that harmonisation with third countries (those outside the EU) would automatically lead to a worse level of protection.

Some interviewees also commented that they are very often subject to regulations in certain jurisdictions that exceed the requirements of the Directive, but that these are still not classified as adequate since they do not constitute a broad, all-encompassing framework. The prime examples of this are the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act in the United States. These impose much more stringent requirements on healthcare and financial services providers than is currently the case in the EU. Similar points were also raised regarding compliance with the Statement of Auditing Standards No. 70 (part of the Sarbanes Oxley Act).

Assigning rights to data subjects was also seen as an issue. The example of a non-European company that wished to establish a data processing centre within Europe was cited. While this move is positive from an economic perspective, from a data controller's perspective it is confusing. Non-European citizens whose data is processed in Europe will be assigned rights that they do not ordinarily have, creating uncertainty as to which legal framework takes primacy.

3.3.4 The tools providing for transfer of data to third countries are cumbersome

Given the above, it is perhaps unsurprising that the alternative mechanisms, in particular BCRs and Standard Contractual Clauses (SCCs), were perceived as a much more positive approach to transfers to third countries. Essentially, these allow (or rather require) data controllers to assume direct responsibility for ensuring the security of the transfer and any other related data transfer.

However, even a contractual approach to data transfer leaves certain issues to be resolved. Most notably, data controllers commented that the processes for accepting standard clauses still varied from Member State to Member State, wasting considerable time for all involved. A clear call was made to: (a) harmonise the procedures for approving contractual clauses, and (b) make mutual acceptance mandatory, so that approval by the DPA in one Member State would make further steps in other Member States unnecessary. This would allow DPAs to make better use of their limited resources, instead of having to conduct an almost identical checking process across each Member State.

BCRs have come under some scrutiny due to the recent initiative whereby they are mutually accepted among a sub-group of sixteen Member States. Under this initiative, a BCR that is prepared, submitted and approved in one jurisdiction is considered as adequate in the other countries in the group. This 'passporting' of BCRs is regarded as counter-productive, since the regulators review them more stringently than SCCs because,

if approved, they will be valid in several countries. However, one interviewee criticised the delay in mutually recognising BCRs, arguing that this should have happened sooner. The lack of a clear framework under the Directive for facilitating this process was sometimes interpreted as a shortcoming within the Directive that placed too much importance on adequacy assessments over more pragmatic solutions.

BCRs were also criticised for being largely only useful for Human Resources data, which is structured sufficiently similarly across organisations so as to be internally consistent and hence suitable for transfer.

The practical application of BCRs has yet to be tested, since a very limited number of data controllers have attempted to implement them. Lack of harmonisation was considered to be the major factor behind the uneven effectiveness of these tools.

3.3.5 The role of DPAs in accountability and enforcement is inconsistent

Enforcing the Directive can be difficult because the damages suffered are often intangible (or sometimes not evident in the short term), it is difficult to assign a value to any damages, and determining responsibilities is complex.

The provisions for remedies and liability in the Directive are quite broad, and in principle allow data subjects ample opportunity to obtain compensation for damages. However, this approach does not function in practice for a number of reasons, including:

- There may not be any immediate damages, such as when confidential data, e.g. credit card numbers, are leaked. As long as the data has not yet been abused, it may be difficult to obtain any compensation, even if negligence on the data controller's part has created a substantial security and privacy risk.
- The extent of damages may be difficult to quantify. To continue the example above: suppose a credit card is abused, but the bank rectifies the problem by refunding the injured party and by issuing a new card. The data subject must still obtain a new card, cancel any payments linked to the old number, notify service providers of changed payment info etc. Clearly, this loss of time and effort has a cost, but how can it be calculated fairly?
- Damages are typically too small to bother with on an individual scale. If 20,000 credit cards must be revoked because a data controller has been careless, 20,000 individuals will have to go through the aforementioned steps. The collective damage is clearly substantial, but it is quite unlikely that any of the individuals involved will undertake any action, since any compensation is likely to be dwarfed by the extra effort and expenditure required to obtain it. The risk of sanctions for the data controller responsible for such an incident therefore remains limited.

If errors are unlikely to have serious consequences, there is no incentive for data controllers to comply with data protection provisions. Enforcement is also perceived to be hampered by the fact that DPAs are poorly funded and overloaded with cases. While the objectives of enforcement remain largely the same across Member States, the power and methods of enforcers vary. In the UK, enforcement is conducted via the judicial system and the regulator has no power to issue fines (although this is currently under review). In countries

where regulators issue fines and are required to recover their own costs, they are effectively incentivised to identify and penalise misbehaviour.

Enforcement strategies reflect legal, cultural and social norms. Interviewees commented that sanction mechanisms are not transparent and it is not clear to the regulated whether there is any particular strategy in place or whether subjects for enforcement are chosen at random. Interviewees also expressed concern at the fact that the some supervisory authorities have the power to enter the premises of data controllers for inspection purposes without extensive formalities, whereas others cannot readily do so. This difference in approaches was not seen as necessarily detrimental. Some saw that regulators were doing their best with limited resources.

In addition, it is clear that enforcement is (and should not be) not the sole responsibility of the DPAs. The Directive generally tasks the DPAs with monitoring the application of the Directive's transpositions (article 28.1). This responsibility includes consultation in the drafting of data protection regulations or administrative measures (article 28.2), powers of investigation, intervention in data processing activities and in legal proceedings (article 28.3), and ombudsfunctions (article 28.4). Thus, the DPA's tasks include enforcement and complaint handling, but also the promotion of good practices.

This mixed role needs to be duly considered: enforcement is one of the key missions of DPAs, and an area in which there appears to be a desire for more coherence between the Member States with regards to the enforcement means available to DPAs, the scope and impact of enforcement actions, and the choice of enforcement priorities. However, this need for greater enforcement consistency should not be to the detriment of the DPAs' other responsibilities in relation to complaint handling and good practice dissemination.

3.3.6 The definition of entities involved in processing and managing personal data is simplistic and static

The relationship between processor and data controller envisaged in the Directive does not adequately cover all the entities involved in the processing of personal data in a modern networked economy. There is uncertainty about when a processor becomes a controller or vice versa, particularly in an online environment where the act of visiting a website might result in cookies being sent from a number of sources scattered around the globe.

Trends toward off-shoring, outsourcing, sub-processing and onward transfer have resulted in companies having to arrange contractual clauses with each and every sub-contractor involved in processing, in order to avoid being in breach of legislative requirements. The bureaucracy involved in reviewing each of the contracts which articulate these relationships (which may have to be re-authorised whenever there is even the slightest change) is clearly a burden for authorities and controllers.

3.3.7 Other minor weaknesses

Our evidence also uncovered a number of other minor weaknesses which although may not be regarded as having the same level of impact as those listed above, nevertheless present difficulties in terms of the practical implementation of the Directive.

Firstly, there is concern over a growing dichotomy between data protection in the first (internal market) and third pillar (law enforcement and judicial co-operation). While the

Directive only covers the first pillar, the consensus seemed to be that a common vision on data protection was needed across pillars. The possible disappearance of the pillar distinction in the future is one reason behind this thinking. More importantly, the existence of special rules that substantially exempt third pillar activities from data protection principles undermines the status of these principles as an important part of the European interpretation of fundamental rights. While some concessions certainly need to be made in the light of third pillar efforts, the current approach to data protection in the third pillar is seen as being too ad hoc and lacking restrictions. While this criticism has been partially addressed through the recent Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation,[82] this does not resolve the continuing distinction between first and third pillar data protection rules and practices. The European Data Protection Supervisor (EDPS) recently raised these issues in an opinion on the Final Report of the High Level Contact Group on a transatlantic data sharing agreement.[83]

Secondly, the Directive expressly encourages codes of conduct that clarify how the provisions of the Directive apply in specific contexts and sectors at both the national and European levels. However, in practice codes of conduct are almost exclusively adopted at the national level, and their popularity varies greatly from country to country. Only two Codes of Conduct have been adopted at the EU level, one by IATA, the other by FEDMA. The Commission expressed its disappointment at the lack of EU level codes in its 2003 First Implementation Report.[84] The interviews for this study gave two main reasons for the lack of success with EU-wide codes of conduct. Firstly, DPAs seemed less interested in reaching a consensus on good data protection practices with the sector, and more interested in unilaterally imposing their own set of rules. Regardless of whether this is a fair statement or not, some data controllers believe that stakeholders and their legitimate interests are not adequately taken into account, and felt that their roles and interests were not adequately acknowledged in the Directive. Secondly, resources to promote and validate codes of conduct were considered insufficient, both within certain DPAs and at the European level. This may be due to a lack of resources or due to different priorities.

In addition, data controllers can in practice become subject to multiple conflicting legal frameworks, either within a country or internationally, without it being clear which rules take precedence. The implications of this confusion can be seen e.g. in the use of personal data for e-discovery (where personal data may be required, or is retrieved as part of a

---

[82] Council Framework Decision 2008/977/JHA of 27 November 2008 *On the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,* Official Journal L 350 , 30/12/2008 P. 0060 – 0071; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML

[83] European Data Protection Supervisor: *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection* Brussels, November 2008; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

[84] *Commission's First Report (2003) on the transposition of the Data Protection Directive*, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT

litigation process and stored longer than necessary) or national security (e.g. via an obligation to retain and provide communications data (i.e. personal data) in order to identify suspects). Another example of a cross border conflict would be the rules regarding whistleblowers, where one set of laws states that a whistleblowers' anonymity should be protected, but the Directive requires that the source is revealed. One example is the SWIFT case, where data could not be revealed under EU law but was required to be revealed under US law. In such cases, the data controller would face liability whatever they did, making responsibilities and liabilities difficult to determine in a fair and transparent manner.

Finally, there is the question of the use of technology to achieve objectives. A positive aspect of the Directive was the fact that it does not specify particular technologies, but interviewees commented that technology could be used to help companies and individuals exercise the rights articulated in the Directive. It was felt that Privacy Enhancing Technologies (PETs) have not been widely taken up, for various reasons. Some respondents commented that use of PETs has been restricted because of the focus on anonymisation technologies rather than a broader definition encompassing pseudonymisation. A vicious circle appears to prevent PET uptake. Companies feel no need to deploy PETs because the regulator does not require their implementation. The regulator does not require PETs because they see no market for suppliers of such technology. Suppliers do not develop PET products because companies are not required to deploy them. The regulators thus know that a viable market for such technology to help compliance does not exist, so they may treat data controllers less harshly for not implementing such technology.

3.4 A summary assessment of the balance between the Directive's strengths and weaknesses

Determining the exact impact of the Directive and weighing the advantages against the disadvantages is a complicated exercise. One the one hand, the Directive is generally credited for improving awareness of data protection issues and of the principles behind good data protection practices, and for creating a legal framework for these principles that has subsequently been implemented in all Member States, including those in which a clear legal framework was lacking. From this perspective, the Directive's impact has been positive.

On the other hand, substantial dissatisfaction also exists on a number of points, most notably on the processes that the Directive has provided to make these principles a reality, and on the question of whether these processes are effective in presenting a real benefit to data subjects and the free flow of personal data in the EU, efficient in choosing the optimal approach to achieve the desired outcomes, and resulting in a real harmonisation of European data protection practices.

Examples of each of these points have been provided above, including the obligation of prior notification as a tool for promoting transparency that has been implemented differently in each Member State (including through simplifications and exemptions); the notions of special categories of personal data which are difficult to apply coherently and

which favour formal criteria for special protection over an assessment of any actual need for such protection; and the extreme difficulty for data controllers to adopt BCRs across the EU despite the presence of a regulatory framework that should be sufficiently harmonised.

Broadly speaking, these weaknesses appear to be indicative of a regulatory framework that focuses not only on the principles of data protection (such as legitimacy, transparency, purpose restriction, etc.) and on the desired outcomes, but also on the processes used to implement these principles (obtaining consent from the data subject, drafting policies, filing notifications, etc.), without adequately considering whether the desired outcome is promoted by these processes, or if these requirements result in an outcome that is proportionate to their burden. At the extremes, this risks creating an organisational culture that focuses on meeting formalities to create paper regulatory compliance (via check boxes, policies, notifications, contracts, ...), rather than promoting effective good data protection practices.

This problem is demonstrated by the perceptions noted above in the February 2008 Eurobarometer study: 64% of data subjects question whether organisations that held their personal data handled this data appropriately, and 84% of data controllers were in favour of more harmonised rules on security measures to improve and simplify implementation of the legal framework on data protection, with only 5% of data controllers believing that existing legislation was fit to handle the increasing amount of personal information being exchanged. Clearly, there is some question as to the effectiveness of existing rules.

It is thus clear that the Directive as it is currently being interpreted, implemented and enforced in the Member States does not fully meet its stated objectives of protecting data subject's right to privacy with respect to their personal data or of enabling the free flow of such personal data within the European Union, even without fully considering the similar need that exists between reliable parties outside the Union. The next chapter will consider how these shortcomings could be remedied.

CHAPTER 4 Recommendations

4.1 Introduction

This chapter presents our recommendations based on the previous exposition of strengths and weaknesses of the Directive. In developing these recommendations, we also highlight examples of similar or relevant legislation, policy or practice from other jurisdictions and regulatory domains to illustrate what might be possible. Examples include the Confianza Online Trustmark in Spain, the Children's Online Privacy Protection Act (COPPA) in the United States, the Korean Information Dispute Mediation Committee (PICO) and new concepts regarding regulatory reform in Australia. We also cite different approaches to regulation in different sectors which may have value or applicability in this domain. Examples include financial services, the 'Better Regulation' agenda and corporate governance.

The evidence from the literature and interviews indicated that many – though not all – of the perceived weaknesses are derived from poor or uneven implementation by Member States. The variability of differing regimes is a double-edged sword: on the one hand, regulators can exploit the latitude to effect practical regulation that has real benefit for consumers/citizens and is better tailored to cultural differences; but on the other hand, this latitude may also be used to create differing bureaucratic processes that present barriers to the Internal Market. When participants in our scenario-based workshop discussed what improvements they would like to see, they overwhelmingly agreed that practical and pragmatic consideration of the rules was required.

A key factor behind our recommendations is the need to 'think global'. Although others have discussed whether striving to harmonise privacy regulations would result in 'a race to the top' or a 'race to the bottom', the approach of regarding other regulatory regimes that do not conform to a European ideal as 'inadequate' and of discarding alternative effective approaches to data protection may be considered outmoded. Future privacy regimes should be interoperable in a global context, and able to provide for the effective protection of personal information across jurisdictions.

Furthermore, growing amounts of personal data being processed means that regulators as well as data protection authorities will increasingly have to act with a strategic mindset. Current process 'ex-ante' orientated mechanisms are arguably no longer valid. Therefore

the regulatory system must actually be made to work for itself, only requiring the intervention of regulators where necessary to:

- encourage positive behaviour where the use of personal data is concerned; and
- enforce the regulatory framework in cases where significant risk of harm or actual harm exists.

Overall, we found that as we move toward an increasingly global, networked environment, the Directive as it stands will not suffice in the long term. The widely applauded principles of the Directive will remain as a useful front-end, yet will need to be supported with a harms-based back-end in due course, in order to be able to cope with the challenges of globalisation and flows of personal data.

However, it was also widely recognised that value can still be extracted from current arrangements and that a lot can still be achieved very quickly by better implementation of the Directive, for instance by establishing common interpretations of several key concepts and a possible shift in emphasis in the interpretation of other concepts. Abandoning the Directive as it currently stands is widely (although not unanimously) seen as the worst option, as it has served, and serves, as a valuable statement of European data protection principles. This overall vision is reflected in how we present the recommendations below.

4.2 Getting the most out of the current system

The future will be dominated by the exchange and use of large amounts of personal data in a global context. While the Directive's approach is not universally efficient or effective in the face of the challenges this future will bring, we recognise that value may still be extracted from a better and more practical implementation of existing rules.

Recommendation 1: A Charter for Effective Interpretation

Common interpretations of certain provisions of the Directive are needed to ensure that it functions optimally in the future. Without undermining the Directive's provisions, a consensus should be sought between Member States on more efficient interpretation, implementation and enforcement of the Directive. This might be articulated in a Charter for European DPAs, and reflect the model recently adopted by Sweden, which, following a review, established a set of regulations using a risk based approach toward the misuse of personal data. This was possible without undermining the existing Directive and the Swedish regulator was convinced that such a route remains legally acceptable without violating the current provisions of the Directive.[85]

[85] This interpretation is based on a statement of the European Court of Justice in the Lindqvist Case (Case 101/01, in particular in §62), which allowed the interpretation of the text of the Directive in relation to transfers of personal data to third countries via publication on a publicly accessible website to take into account the intention of the Community legislature and to the possibilities for the Member States to restrict the scope of a series of provisions of the Directive, e.g. in order to protect the rights and freedoms of others (Art. 15 of the Directive)

Such a Charter would:

- Encourage the use of a risk based approach to the application of the rules, focusing on acts of data processing where harm can reasonably be expected. In the Swedish model, most everyday forms of non-structured personal data processing that are common nowadays are exempt from a great many of the procedural regulations.[86] Processing of personal data is not permitted if it involves an improper intrusion into personal integrity. Explanatory comments to the legislation help understanding of what this means in practice.
- Reducing the burden of the notification obligation, by making non-notification the general rule, rather than the exception, making broad use of the possibilities of Article 18 paragraph 2 of the Directive; and by ensuring that any remaining notification obligations remain sufficiently light and pragmatic. Current notification obligations were often seen as too burdensome and formalistic, with little or no benefit to any stakeholders. While transparency of data processing should remain a fundamental principle, notification should be required only in cases of notable risk or harm, or when transparency cannot be adequately ensured via other means. In that respect, notification can be reconsidered as a useful tool to assist DPAs in their enforcement duties, rather than as a transparency enhancing device, by providing the DPAs with essential information on acts of data processing that entail notable risk or harm. In particular the possibility of replacing notification by the appointment of a personal data protection officer (Art. 18.2 of the Directive) should be emphasised. Member States should be stimulated to amend their national data protection law in this respect, thereby trying to harmonise the notification requirements and procedures as much as possible between Member States.
- Ensure that BCRs can be more easily used to ensure the legitimacy of personal data transfers to third countries, rather than relying on determining the adequacy of entire countries. This could be achieved by formalising the measures currently being developed by certain supervisory bodies, with associated guidance as to their common understanding, and should be designed so as to maximise common acceptability across Member States. Care should be taken to maintain incentives for the private sector. The current attempts to introduce a system of mutual recognition between Member States are partly successful but run into problems, notably because some of the national transpositions have not included a sufficient legal basis for adopting such a system. Member States should be persuaded to amend their national personal data protection law accordingly to allow such systems to operate in practice.
- Improve accountability in the case of infractions that could cause significant damages either because of the nature of the personal data or because of the

[86] As summarily described in the *10th Annual Report of the Art.29 WP*, p. 112; see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/10th_annual_report_en.pdf; also briefly communicated on http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/andringar-i-personuppgiftslagen/ (Swedish only).

number of affected data subjects. In addition to the existing provisions of the Directive this could be done by:
    - introducing breach obligations incumbent on the data controllers under Article 23 of the Directive, which can include mandatory disclosure in certain cases, either to the DPAs or to the data subjects if the latter would reduce the risk of actual harm occurring, and which should at least include an obligation to mitigate damages and to assess existing practices to eliminate/reduce the risk in the future;
    - ensuring that DPAs are able to impose suitable sanctions on data controllers under Article 28 paragraph 3 of the Directive, which should also include broad investigative measures and operational measures.
- Work towards helping data processors to meet their transparency requirements more effectively, such as via better notices on websites. This might include layered privacy notices, which would allow users to follow links to further or more in-depth information regarding topics of interest. Layered privacy notices would take up less screen space and would not compete for the attention of the viewer, and might also include a description of the risks that personal data might be exposed to in the specific context of the request.

We reiterate our assessment that a new Directive is not the right choice of legal instrument to achieve these shorter term aims, as a full review of the Directive is not necessary to achieve these goals and would likely take a substantial amount of time. A route to a more pragmatic understanding should be further considered without having to wait for a substantial review of the Directive itself, as proposed further below.

Recommendation 2: Work to improve the effectiveness of the Adequacy Rule and facilitate the use of alternatives to the Adequacy Rule

The study shows that the Directive's focus on adequacy assessments and the strategies to achieve this are inefficient and insufficiently productive in an increasingly globalised data market. Key economic trading partners are not covered by adequacy findings, which mean that alternatives should play a crucial role in practice. When these are not easily available, non-compliance is de facto encouraged.

The promotion of alternatives – such as SCCs and BCRs – should become a greater priority. The use of these alternatives should be facilitated for data controllers in any Member State, as was already noted above.

In addition, it was noted by several interviewees that current adequacy assessments were not sufficiently effective, focusing mostly on a review of regulations and declared policy, rather than on the effectiveness of data protection. If the credibility of the adequacy assessment system is to be maintained, assessments should consider whether the principles put forward by the Directive are achieved in practice, which includes issues such as the actual independence of DPAs and court rulings on data protection issues, the availability of sufficient means to allow DPAs to operate in practice, and the existence of actual enforcement actions.

Recommendation 3: Clarify terms on privacy norms, privacy-by-design and business understanding

The Article 29 Working Party should work towards the following clear Opinions:

- On privacy norms and standards, indicating that certain measures might be met by following best practices or standards (e.g. emergent ISO initiatives on privacy).
- On the role of "privacy-by-design" as a requirement for any new technology under the current Directive.
- On business understanding/business models to encourage a more flexible and practical understanding of the term "completely independent supervisory authority", with the understanding that most private sector organisations are trying to comply with legislation and that interaction with industry does not necessarily compromise the independence of DPAs.

Recommendation 4: Develop common enforcement strategies

The London Initiative of DPAs should develop a common enforcement strategy for independent supervisory authorities, crystallised in an instrument such as a non-binding Memorandum of Understanding. This should be published and endorsed by the EDPS so that the standards used to judge the regulated are clear. This strategy should take into account legal and cultural traditions and contexts across the Member States and use these differences to its advantage.

Recommendation 5: Achieve broader liaison with stakeholders

The Article 29 Working Party should liaise more systematically with business representatives, third sector and NGO communities, and the perspectives of NGO representatives and citizen organisations should be more explicitly taken into account.

Recommendation 6: Development of more suitable privacy policies

The analysis showed that the use of privacy policies has become a standard practice, but that this does not result in much added value for data subjects, due to the often inaccessible and/or incomprehensible nature of such policies. This problem is exacerbated when privacy policies are employed by data controllers as a means of obtaining the data subjects' consent. It is questionable whether real consent as defined by the Directive can be obtained through such notices.

DPAs, facilitated by the EDPS, should be encouraged to develop clear guidelines for data controllers on communicating their policies to data subjects. This could be done via 'off the shelf' privacy policies, comparable to the Creative Commons[87] model of Intellectual

[87] See Creative Commons – *About - Licenses* http://creativecommons.org/about/licenses/

Property Right (IPR) licences. In a Creative Commons model, certain standard types of licences are developed which can be communicated to end users through short, easy to understand descriptions (e.g. "attribution", "non-commercial", "no derivative works",...). A comparable approach could be adopted with regard to privacy policies, by providing summary notices based on such standardised descriptions. These should be relatively easy for interested consumers to understand.

Recommendation 7 – Strengthened support for exercise of rights

The DPAs, in conjunction with civil society stakeholders should work with consumer protection organisations (e.g. the European Consumers Association, BEUC) to institute a national network of grass-roots level 'accountability agents' to support citizens in the exercise of their fundamental rights. Although similar activities are currently undertaken by DPAs, resourcing constraints suggest that a more localised network would be a better approach, having a more widespread presence. These local accountability agents would act as another means for citizens to exercise their rights within existing arrangements. Staff would be knowledgeable both in the legislative context (such as subject access rights, matters of legitimacy and proportionality) but also the realities of modern socio-economic uses of personal data, and would be informed as to where to go for more information. They would represent the first stage in an enforcement 'triage' freeing up resources for DPAs to focus on more strategic matters.

4.3 Making European privacy regulation internationally viable for the future

4.3.1 Increasing momentum for change

We have noted above the need for a more in-depth review of the Directive's approach and provisions in the longer term. Since our study began, we note that appetite for reviewing the suitability of the Directive has increased. Specifically, this can be seen with:

- The comparative assessment study commissioned by Directorate General Justice, Freedom and Security in June 2008, which indicated that the "time was right for an open reflection" and asked for "…guidance on whether the legal framework of the Directive provides appropriate protection or whether amendments should be considered in the light of best solutions identified"[88]
- Remarks by Jacques Barrot noting that "…we will have to reflect on the possible need for modernising the legal framework"[89]

---

[88] Directorate General Justice, Freedom and Security Specification for Invitation to Tender JLS/2008/C4/011 *Comparative study on different approaches to new privacy challenges, in particular in the light of technological advances* p 5 available at: http://ted.europa.eu/udl?uri=TED:NOTICE:117940-2008:TEXT:EN:HTML

[89] Speech by *Jacques Barrot to the European Parliament on the occasion of the Third Data Protection Day* 28th January 2008; http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/27&format=HTML&aged=0&language=FR&guiLanguage=en (in French) originally: « Nous devrons réfléchir sur l'éventuelle nécessité de moderniser

- The launch of a large open consultation in mid-2009 on the future of the Directive.[90]

4.3.2 Effecting reform

The process of amending the regulatory framework that has built up around the Directive is highly politicised and its outcome is uncertain. This is due to a variety of factors, most notably the relationship with other legislative instruments, cultural differences and perceptions of data protection between the Member States, and also the question of choosing the most effective regulatory instrument when considering the potential influence of future reform regarding the 1st /3rd Pillar division.[91]

It is thus clear that this study and its recommendations should be considered in a broader and more encompassing consultation in the future to determine a new longer term vision for European data protection regulations. Nonetheless, through the smaller scale consultations of key stakeholders in the public and private sector (including data controllers, lawmakers and DPAs) that have been performed in the course of this study and on the basis of the analysis described above, we present our own recommendations for a coherent, more effective and more efficient approach to data protection below.

These recommendations are aimed at facilitating cost effective compliance for data controllers, at increasing the effectiveness of data protection for data subjects, and at ensuring that DPA resources can be well targeted. We would like to reiterate that this presents a clear opportunity for Europe to take the lead on privacy protection and once again, as was done with the original Directive at the time, establish a reference model for many years to come.

Recommendation 8: That the upcoming consultation and review consider the following proposed regulatory architecture

Based on the findings above, the study team recommends that the upcoming consultation should consider pursuing a regulatory architecture which:

---

le cadre juridique existant au regard des nouvelles technologies et répondre aux nouveaux défis dont on parle aujourd'hui, que nous ne pouvons plus ignorer et que nous devons absolument relever. »

[90] Speech by *Jacques Barrot to the European Parliament on the occasion of the Third Data Protection Day* 28th January 2008; http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/27&format=HTML&aged=0&language=FR&guiLanguage=en (in French) originally : « La situation actuelle néanmoins doit être améliorée et je peux vous dire que j'ai l'intention de lancer une large consultation afin de renforcer la protection des données. »

[91] Hustinx, P., *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme* for better implementation of the Data Protection Directive Opinions of the European Data Protection Supervisor Official Journal of the European Union C 255 27th October 2007 p 2 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

- is pragmatic and outcome-focused for data subjects and data controllers also taking into account the limited resources available for assessing and enforcing compliance;
- is internationally viable, given a range of differing privacy regimes and the understanding of uses of personal data being international and cross border;
- is consistent with the Better Regulation agenda, namely being self-managing, focusing on a regulatory 'light touch' but with sufficiently powerful tools for enforcement and due diligence by ISAs;
- builds upon the strengths identified in the study of a 'principles based approach' rather than an excessive reliance on the general effectiveness of formal processes to protect individual privacy; and
- addresses the weaknesses of un-harmonised, confusing and contradictory implementation.

We believe that such a consultation will be, in and of itself, educative in stimulating discussion regarding the weaknesses our report has identified and potential avenues to address them.

We emphasise that our recommendations aim to provide for a more effective and outcome oriented protection of the right to privacy. Our research indicated broad agreement that a human rights based approach is important and should be retained. Furthermore, instituting a system which surrenders this right would fly in the face of a number of important international and legal instruments, and risks endangering the clear societal benefits created by a solid privacy protection framework. Having said that, what does need to be made clearer is the extent to which the practical exercise of this right is fungible. If the right is exercised absolutely by individuals, then there may be important consequences for the individual in terms of broader economic and societal benefits. However, this decision remains to a large extent up to the individual.

Objectives of proposed regulatory architecture

Any governance architecture must clarify and explain its desired outcomes. In the case of the Directive (or a future re-casting thereof), one way of doing this is by examining the roles, rights and obligations of the different stakeholders.

- From the data subject's perspective, the regulations should provide for suitable and effective protection against direct or indirect physical, economic or social damage or distress caused by the disproportionate or unauthorised use of their personal data. This should be tempered by the realistic assumption that, although it is possible to exercise the right to be 'let alone' to a large extent, there may be consequences to doing so, in terms of the opportunities to participate fully in the information society. This protection can most notably be afforded by ensuring that the regulatory framework provides clear and realistic opportunities for enforcement, including through the definition of clear data subject rights, coupled with the accountability of the data controller.
- From the data controller's perspective, the regulations should define the outcomes to be achieved through suitable data protection practices, and declare the data

controller's accountability when these are not realised. The extent of the efforts to be imposed on the data controller to ensure that the Outcomes are met should be dictated by criteria of potential harm to data subjects. We have already indicated the complexity of trying to define harms specifically, but nevertheless it is possible to identify some initial types of harm that might be considered at a minimum:

- Economic harm – such as financial damages suffered as a consequence of identity theft, loss of earnings, financial or economic discrimination etc
- Personal, physical or psychological harm – such as becoming a victim of a crime against the person or discrimination as a result of personal data mismanagement
- Social damage – such as damage to reputation and social exclusion due to mis-use of personal data

There is considerable debate as to whether 'damage to society' might constitute a separate form of 'damage', to be considered separately from individual harm. Although there are clear implications in terms of undermining of trust and confidence in society by the unconstrained use of personal data, understanding of this issue goes to the heart of whether society as a whole could be considered a victim when individuals are harmed, or whether harm should be considered to exist if no individual victims can be readily identified, and whether rules should consider societal risk as a factor to determine rights and obligations. This is related to the debate over whether supervisory bodies should be tasked with protecting individuals against the unlawful processing of their personal data (it being understood that this will also benefit society as a whole), or whether they serve a broader purpose as protectors of privacy in general. In this respect, and subject to the outcomes of broader European scale consultations, it might be more practicable to begin by carefully identifying forms of harm against individuals.

- From the perspective of ISAs,[92] the regulatory framework should ensure that they have the required means and competences to ensure compliance, both by investigating data protection practices and enforcing the framework against data controllers who do not meet the required outcomes (i.e. ensuring the accountability of data controllers for their actions), and by ensuring that appropriate tools are available to data controllers so they can achieve the required outcomes.

Matching general principles to real outcomes

In line with the ideals of Better Regulation, the architecture of European privacy governance may be organised around a principles based 'front-end' and a harms based 'back-end', consistent with a broad approach to the management of risk applied to the privacy context, with a focus on preventing the misuse of personal data wherever possible, and ensuring that strict enforcement is possible when misuse does occur. General Data Protection Principles, ("General Principles") similar to those currently present as identified

[92] We use the OECD terminology Independent Supervisory Authorities (ISAs) deliberately in this context to reflect global thinking

in the preceding chapters, would be defined along with the desired outcomes on the basis of "prevention is better than cure".

In the resulting regulatory approach, European level legislation should lay out General Principles and desired Outcomes. The appropriate means to achieve these General Principles consistent with desired Outcomes should however not be imposed as generally binding obligations at the European level, as this would not be consistent with a risk based approach. While some possible tools and instruments for meeting the General Principles and Outcomes can be defined at the European level – much as e.g. notification and the use of data protection officers are currently already defined as tools in the Directive, albeit without explicitly stating the objective that these serve – the selection of appropriate means for specific acts of data processing can be determined locally, either via national data protection rules (generic or sector/context specific) or via co-regulation (e.g. established via dialogue between ISAs and sectoral representatives). Data protection practices can then be assessed on the basis of whether the desired General Principles and Outcomes are met, rather than on the basis of a process orientated review.

To summarise, this approach would consist of:

- Defining data protection goals at the European level (General Principles and Outcomes);
- Choosing suitable tools or instruments locally; and
- Ensuring that enforcement is possible whenever Principles are not observed or Outcomes are not met, and that data controllers can be held accountable when harm is caused because of their non-compliance.

General Principles

Achieving this in reality would mean that the Directive is re-cast as an articulation of General Principles and Outcomes. The detail of implementation measures would sit elsewhere.

The General Principles would represent a set of criteria which data controllers, public and private, should attain. They are the ultimate means by which ISAs are empowered to act. As demonstrated earlier, these are already generally consistent elsewhere in other international norms. These General Principles also ought to define expectations and responsibilities for data subjects and regulators.

- Legitimacy – i.e. defining when personal data processing is acceptable
- Purpose restriction – ensuring that personal data is only processed for the purposes for which it was collected, barring further consent from the data subject.
- Security and confidentiality – specifically by requiring the data controller to take appropriate technical and organisational measures
- Transparency – that appropriate levels of transparency are provided to data subjects
- Data subject participation - ensuring that the data subjects can exercise their rights effectively
- Accountability – that those processing personal data would be held accountable for their actions according to the Outcomes

The principles should be ratified, agreed and may then be articulated in different ways depending upon the context and type of stakeholder.

Implementation

A set of implementing instruments, tools or policies consistent with a risk based approach would form the 'back-end' for the achievement of these principles.

Further discussion will be required to clarify how regulation can appropriately consider and address the presence of risk. Some possible criteria or avenues for determining the risk involved in specific categories or acts of data processing would be:

- the scale on which personal data is processed (e.g. more stringent requirements could be applied to the processing of personal data in relation to 500,000 data subjects than in relation to 500 data subjects)
- the privacy sensitive nature of the data being processed, and more specifically whether the nature of this data causes it to be more likely to result in (increased) harm, considering the full context of the data processing (e.g. the processing of health-related information, racial information, etc)
- the field of activity of the data controller, as a proxy for the risk of harm (e.g. financial services, health care, legal services)

While risk is often difficult to determine ex ante, the strength of a risk based approach lies precisely in the need to evaluate how risk changes dynamically as data processing practices evolve (e.g. because of changes in the scale of data processing, or expansions to other fields of business). As practices change (and as risk changes), the measures needed to ensure compliance will evolve as well. In this way, a risk based approach stresses the importance of implementing a sound data protection culture, rather than on one-off compliance formalities.

The need to appropriately consider risk as the predominant consideration in determining in what way the fundamental right to the protection of personal data as specified in the European Charter of Fundamental Rights may be best safeguarded supports this right without the imposition of inappropriate or disproportionate burdens. A risk based approach should thus not be interpreted as arguing for the application of regulations only when there is a sufficient risk of harm.

Regulatory focus at the local level would thus necessarily be on implementation, since if the desired Outcomes of treating personal data are properly described and the General Principles are carefully articulated, then these will be more readily 'self-enforcing' (on the basis that data controllers will be able to identify a suitable course of action more easily). The use of clear cut behavioural rules is a common legislative technique in other sectors, for example in competition law, where there is a clear distinction between obvious infringements ("bright line" law) versus other more ambiguous situations which are more dependent upon the exact context of the circumstances ("rule of reason").[93]

[93] Jones, A., Sufrin, B. and Smith, B. *EC Competition Law: Text Cases and Materials* Oxford University Press 2007 Oxford p967

Different means may be seen to establish accountability against this regime. For commercial organisations that operate on the basis of economic incentives, these could be driven by regulations and instruments consistent with such drivers, including co-regulation. For the public sector, this might rely upon direct requirements such as the publication of statistics, league tables or other information. At a European or national level, the regulator might determine that certain organisations must adopt certain tools, depending upon the degree of risk. For example, large financial companies may be required to employ all or a number of these means of compliance, whereas a small micro-business may be only required to use the bare minimum after indicating they are knowledgeable about the General Principles. Examples of such means may include:

- **Privacy Policies** – A privacy policy should communicate how an organisation intends to achieve the Principles set out above and provide sufficient information to be used, when necessary and appropriate, for audit, review and investigation by a regulator. It would be up to the organisation to determine what an appropriate policy would look like, with the expectation that this would be commensurate with the risk that personal data is being exposed to and compliant with locally defined requirements. The change from current practices is that the privacy policy would not be seen as an instrument to assure transparency, but rather more clearly as a means to provide for accountability between the organisation and the regulator (unlike privacy notices which serve as transparency tools, as will be noted below). Policies might be specific to certain uses of personal data (if deemed to be particularly risky) or cover the entire organisation. For smaller organisations, the regulator might provide off the shelf policies which may be easily tailored to suit. The example of Creative Commons licensing is a case in point in this respect. A focused view of accountability must be taken, however. Thus, it should not be possible for an organisation to be 'accountable' to a privacy policy which permits use of personal data contrary to the General Principles or Outcomes.
- **Privacy Notices / Statements** - if carefully designed, would support objectives of transparency by alerting individuals as to what is being done with their personal data. However, these need to be more accessible than is currently often the case. They would need to be tailored to the circumstances and may also operate on a 'by exception' basis, consistent with the risk based approach outlined above. This would build upon current consumer expectations; e.g. when making purchases on-line, it is a given that personal data will be processed for the provision of products and services, so the privacy notice should focus on any unusual uses or circumstances which may affect them. Individuals generally also expect as a given that their personal information will be kept secure and that they would have access to it and the ability to change or remove details, as a right – removing this obligation would help make notices more pertinent without lengthy irrelevant information informing consumers what they already know or expect; the latter could easily be integrated into privacy policies. Notices might also take advantage of the various ways in which individuals make decisions, for example by referring to a known 'rule of thumb' or other heuristic that would enable consumers to speedily make a meaningful and constructive choice or comparison. The privacy notices may also vary depending on context or situation - for example, deploying

different notices depending on whether a transaction is being entered into, as compared to simply browsing or otherwise interacting with a website.

- **Chief Privacy Officers** – the Chief Privacy Officer role may be identified as an alternative to a privacy policy, there mainly to provide for accountability within an organisation. Regulations should be designed that would make Chief Privacy Officers personally responsible and/or criminally liable for willingly engaging in risky, unscrupulous or irresponsible behaviour by their organisations regarding the use of personal data. This would be comparable to the model of the Chief Privacy Officer in certain organisations in the US, which hold real decision making and enforcing power and are highly respected both within their organisations and by regulators and DPAs.
- **Registration** – when this is justified based on a prospective analysis of risk, data controllers in organisations could be required to register a set of simple summary and pragmatic data with the ISAs to facilitate enforcement when intervention is required (i.e. in case of investment or enforcement actions). This would have the secondary benefit of providing a revenue stream for the ISAs. Again, it is crucial that an understanding of risk is applied in determining if a registration is required and how far it should go– the fees might be scaled according to the likely risk that personal data is exposed to (e.g. in terms of the sensitive nature of the data or the scale on which data is collected (number of data subjects). This may be based on the organisation's own estimates and expectations, permitting intervention if this information is deliberately misleading or incorrect. It would not be appropriate to introduce blanket notification requirements to be applied to all data controllers irrespective of risk.
- **Codes of Conduct** – would build on models that are in existence now, such as the Direct Marketing Association code of conduct, and would probably (although not exclusively) be sector specific. The advantage of Codes of Conduct is that they can be tailored to specific contexts and may be generated from the ground up or driven by organisations with a thorough understanding of data protection issues in a specific sector. Aside from current examples, such as IATA and FEDMA, Japanese Personal Information Protection Organisations are another example of a code of practice based system. In India, the Data Security Council of India (DCSI) is also looking at self-regulatory code. In the UK, the Advertising Standards Authority (ASA) Code of Advertising Practice (CAP) is an interesting example as it illustrates how a self-regulatory body might operate in the drafting, revision and publication of codes. Furthermore the regulated contribute toward the ASA through a levy and sanctions are undertaken by independent adjudication.
- **Corporate Governance Code** - consistent with current thinking in Corporate Governance, a code might developed as a non-binding set of rules or recommendations for organisations to follow which are not mandatory, but with which organisations must comply or explain why they do not. They could be developed and published by the regulator. This approach has been recognised to

'fit well with differing legal and national frameworks'.[94] Responsibility for the explanation of non-compliance would rest with the organisation, as would the quality of the measures taken to comply with the code. Thus, accountability must remain guaranteed, in accordance with the proposed General Principles.

- **Privacy Reporting/Accounts** – in a similar way that accounts for publicly listed companies are published and must be signed off by authorised parties, it would be possible to require that certain high risk organisations (e.g. in the financial or health care sector) should periodically publish data reflecting their use of personal information, or report incidents related to misuses, losses, breaches, or complaints. These might be signed off as a 'true and accurate picture' by suitably regulated third parties. This requirement should be different depending upon the risk that personal data is exposed to; for example a small micro-business with a few customers should not have to publish such accounts, but a large multi-national healthcare concern would have to publish annual records. As ever, risk is the critical factor in determining which of such measures is adopted. This could prove to be a useful tool to pre-emptively identify and address risks, including by identifying incidents that have not (yet) resulted in clear harm to any individual. In this way, data controllers would be incentivised to find solutions to potential problems, rather than waiting to see if a problem causes sufficient damage (including reputational damage to the data controller) to warrant intervention.
- **Standards** The use of standards to protect privacy is beginning to gain ground. Standards provide additional support for accountability, by permitting a regular review of whether those that have agreed to abide by certain rules do so. This is only possible, however, if organisations become compliant (i.e. get certified) against a standard, rather than merely implementing the best practice. ISO 27001 Information Technology – Security Techniques – Information Security Management is a suite of standards describing best practice in setting up and running an information security management system. Although the best practices evident in this standard have been applauded, it is relevant in the context of the protection of privacy by virtue of providing a framework for meeting the legal requirement of appropriate technical and organisational measures to protect personal data. With this in mind, Working Group 5 on "Identity Management and Privacy Technologies" of the ISO/IEC Joint Technical Committee (JTC) 1 Sub-Committee 27 has been leading the investigation into the viability of a privacy technology standard.
- **Kite-marks / Trustmarks / Seals** – The use of trustmarks and privacy seals is increasingly seen as a viable alternative or supporting mechanism for the protection of privacy. Trustmarks or seals are effectively a filtering and rating mechanism that permit consumers to exercise choice in the market, using the presence or membership of a Trustmark scheme as a criteria in their decision to enter into a commercial relationship with a supplier (usually online) involving their personal information. In that sense, such marking schemes serve a similar

[94] Statement of the European Corporate Governance Forum on *The Comply or Explain Principle* available at: ec.europa.eu/internal_market/company/docs/ecgforum/ecgf-comply-explain_en.pdf

transparency purpose to the privacy notice suggestions above, in addition to having a clear accountability element (as data controllers are expected to adhere to the requirements for using a given mark). There is a school of thought which considers whether such schemes are effective or if they are largely unused by consumers. The most well known scheme in this area is TRUSTe, which is a system based on a voluntary scheme. Other examples from the US include the Better Business Bureau Online, the American Institute of Certified Public Accountants Web Trust program and Secure Assure. As a European example, in Spain, Confianza Online was set up in 2004 to address trust in commercial communications in electronic interactive media and contractual aspects of business to consumer transactions. It created the Sello de Confianza. This seal program covers how a business treats personal data as part of its overall reputation and measures how that affects customer confidence in dealing with member companies. The code was registered at the Spanish Data Protection Register (supervisory authority), and as of September 2007 there were 160 member companies. Other examples of broader seal programs include PriceWaterhouseCoopers' BetterWeb seal.[95]

- **Privacy Impact Assessments** – as a way of assessing the likely impact of measures upon privacy, the use of these could be encouraged by ISAs.[96] Similar to the Privacy Reporting/Accounts tool mentioned above, this could be a useful approach to force higher risk data controllers in the public or private sector to conduct a clear prospective risk analysis of their data processing plans, serving the same purpose of encouraging responsibility and respecting proportionality of personal data processing. Privacy Impact Assessments (PIAs) might be especially suitable for the public sector, where large scale investments might affect entire populations. They might also be considered part of the standard European Impact Assessment process when developing policy measures that may have financial or regulatory impact.[97] The mandatory use of PIAs has already been introduced in the USA under the terms of the E-Government Act of 2002.[98] Similarly, their broader use has been examined in the UK,[99] Canada[100] and Australia.[101]

---

[95] Joseph, Bostick and Slaughter Web Assurance Seals – Are they All Alike? A look at web-trust and other Web Assurance Seals *Journal of the International Academy for Case Studies* Volume 11 Number 4, 2005

[96] For an example of one approach see Office of the Privacy Commissioner of Canada *Assessing the Privacy Impact of Programs Plans and Policies,* October 2007 available at http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf

[97] European Commission – *Better Regulation – Impact Assessments* http://ec.europa.eu/governance/better_regulation/impact_en.htm 2009

[98] See Department of Homeland Security; http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm and Department of the Interior; *Privacy Impact Assessments* http://www.doi.gov/ocio/privacy/pia.htm.

[99] See Information Commissioner's Office: *Privacy Impact Assessment Handbook* http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

[100] See Office of the Privacy Commissioner of Canada; *Privacy Impact Assessments* October 2007 available at http://www.privcom.gc.ca/pia-efvp/index_e.asp

[101] See The Office of The Privacy Commissioner, Australia; *Privacy Impact Assessment Guide:* August 2006 available at: http://www.privacy.gov.au/publications/pia06/index.html

- **Technology –** technology has a clear role to play in enforcing policies and supporting compliance with the principle of security and confidentiality. However, this should only be in the context of the greater objectives of achieving the Outcomes through compliance with the General Principles.
- **Breach notification** - as we described in Recommendation 1, breach notifications could be a useful tool to facilitate enforcement and achieve desired Outcomes under certain circumstances. The judicious use of breach notification measures would help to ensure accountability by incentivising organisations to meet the Outcomes (by shaping market behaviours). Studies have explored whether there is a correlation or causal link between security / privacy notifications and market impact.[102] They also support the exercise of rights by individuals (by permitting them to make a choice regarding which organisation uses their personal information based on the information provided in the notice). However, Breach Notifications must be carefully scoped – they should not be used for every incident since this would devalue them.
- **Alternative Dispute Resolution (ADR) –** ADR measures are regarded as a useful means of permitting consumers / citizens to exercise their rights more easily. The principle is that they permit easier access to justice without having to go through the complex, time consuming and uncertain judicial system. They may be particularly useful in consumer contexts where relatively small levels of economic damage are being considered and where it would be more costly to pursue a case through traditional judicial means. One well-known ADR system is Squaretrade, which is an alternative dispute resolution system used by eBay. In Korea, the Korean Information Dispute Mediation Committee (PICO) is another relatively well-known ADR system, founded to protect personal information in the private sector and complaint handling regarding infringement of the Act on Promotion of Communication Network Utilization and Information Protection. This committee has a broad set of members from industry, academia, civil society and government. It was created with the intention of being a quick and convenient way to mediate disputes through an offline or online dispute resolution system. Mediation is free of charge. Finally, ECODIR and CCFORM are also of interest. ECODIR is a pilot project funded by the European Commission providing online consumer conflict resolution services. CCFORM is another pilot project looking at developing an online multilingual complaint form and best practice business process. In that respect, ADR can be used as a means to facilitate accountability towards data subjects. However, the benefits of ADR systems may be ephemeral, and the effectiveness and impact of such schemes thus needs to be carefully considered. A 1996 study conducted by RAND's Institute for Criminal Justice as part of a requirement for the US Civil Justice Reform Act (CJRA) on early mediation and case management indicated that:

  "…once litigation had begun, referral to ADR was not a panacea, nor was it detrimental. Neither time nor costs nor lawyer views of satisfaction

[102] Acquisit, A., Friedman, A., Telang, R., "Is there a cost to privacy breaches? An event study" *Fifth Workshop on the Economics of Information Security* Cambridge, UK (2006) Draft – very preliminary paper available at:

or fairness changed significantly as a result of referral to any of these programs. . . .[103]

- **Targeted information campaigns** – as a way to inform individuals about specific issues or promote understanding of the use of certain instruments. Such campaigns would need to be carefully co-ordinated and success monitored. They might take advantage of the role of the media in publicising certain events (for example by citing a recent data breach as an example of what not to do) and they should be designed according to models of individual understanding and perception of risk currently being evaluated in the fields of behavioural economics. Information campaigns will need to tread a fine line between maximising understanding and permitting data controllers to specifically abrogate their responsibilities for choosing the correct instrument according to an appropriate dynamic evaluation of risk.

Using these instruments it would be possible to further foster a market for personal data protection, and help to break the deadlock of an approach to compliance based on adherence to processes and 'box ticking'. The market would thus be able to judge the performance of an organisation, incentivising organisations to improve their performance, thereby creating competition. A virtuous circle would be generated by enabling differentiation and assessment according to the quality of these measures and the extent to which they match or exceed those of peers or what may be judged as standard business practices for a specific sector. For example, in a similar way that publicly listed companies currently can be credit rated by Moody's or Standard and Poor's, it may be possible to develop similar processes based on approaches to privacy, with these measures as the means for rating organisations.[104]

Governments and regulators could act in a number of ways to support this, including by:

- stipulating minimum standards for certain sectors; and
- using purchasing power by specifying minimum criteria when undertaking procurement

Establishing clarity on responsibility for those collecting or using personal data in the selection of these instruments would also help in part to counteract a potential perception of a conflict of interest between ISAs and those being regulated. If ISAs refrain from deep involvement in the guidance or the drafting of these instruments then clarity when it comes to enforcement against these tools may be promoted.

As recent events in the global financial system have demonstrated, however, a regulatory approach of 'letting the market decide' must be supported by strong enforcement and accountability to make sure that those being regulated are not allowed to get away with

[103] Kakalik, J. S. Dunworth, T., Hill L. A. et al (1996), *An Evaluation of Mediation and Early Neutral Evaluation Under the Civil Justice Reform Act* MR-803 (RAND, Santa Monica) 1996

[104] Abrams., M, Crompton, M. and Cowper, C. *A possible way forward: Some themes and an Initial Proposal for a privacy and Trust Framework*; A working Paper for the Privacy and Trust Partnership November 2007

irresponsible and risky behaviour.[105] Enforcement measures will thus need to be consistent with a growing appetite for strong and effective powers to intervene.

Enforcement

Enforcement will be necessary to support the use of these tools. ISAs must be able to intervene when misuse has been identified, either pre-emptively (for example, a large telecommunications company with a simple 'off the shelf' privacy policy would alert the ISA to a likely mismatch between the realities of their use of personal data and the measures taken to comply with the General Principles), or after the fact, when actual harm has occurred.

Conditions for imposing fines, liabilities and sanctions should be clearly published. The criteria for issuing fines might be according to a proxy for the extent of risk –for example, numbers of personal records involved, or whether the incident involved actual harm (and if so what sort of harm). The Federal Trade Commission (FTC) in the United States uses the following criteria:

- Egregiousness of conduct – was the breach the result of carelessness; could it have been avoided, what were the measures in place to protect personal data – what could the company reasonably have done to prevent the incident?
- Number of consumers affected
- Monetary loss (to the consumer)

In a similar manner, the UK Financial Services Authority (FSA) uses the following criteria[106] when deciding whether to issue fines:

- The nature, seriousness and impact of the suspected breach
- The conduct of the person after the breach
- The previous disciplinary record and compliance history of the person

ISAs may act strategically by selecting a single sectoral representative or they may respond to consumer complaints based on an assessment of the extent to which action would contribute toward the achievement of Outcomes. Regulators may act as a second order player in enforcement, leaving sector specific regulators as the lead and acting in an advisory capacity. Ultimately, ISAs will need to act in a more strategic manner to achieve real outcomes, rather than meeting targets for completed investigations.

Revenue from civil sanctions should be returned to those affected where identification is possible and reasonable. An example is the Financial Services Compensation Scheme (FSCS) in the UK, where retail consumers and SMEs can be paid compensation for harms depending upon greatest need. Fines should not be a source of revenue for the regulator

---

[105] "*Barroso hails spirit of convergence at Brussels Summit"* The London Summit 2009 available at: http://www.londonsummit.gov.uk/en/summit-aims/timeline-events/european-leaders-3

[106] UK Financial Services Authority: *Decision Procedure and Penalties Manual Release* 070 Section 6.2 available at: http://www.fsa.gov.uk/pubs/hb-releases/rel70/rel70depp.pdf (October 2007)

since this would create perverse incentives that might drive inappropriate enforcement behaviour. Criminal sanctions might also be applied for serious breaches.

The role of the Independent Supervisory Authority

The role of the ISA would thus evolve from being a process orientated checker to a strategic advisor and, above all, an enforcer. This is only natural given the exponential increase in personal data likely to be processed globally, and the existing resource constraints of European regulators.

The complaint handling role of ISAs may no longer be as strategically appropriate, since trying to deal with all complaints could become overwhelming given the quantities of data being processed. Instead, ISAs would take action according to a set of criteria designed to help them decide if their involvement would help enforce and achieve the high-level Outcomes. Organisations would be expected to see it lies in their best interests to handle complaints quickly, since this would ultimately be rated as part of any market based system, and since inadequate handling of complaints could result in enforcement actions. However, there may be a role for consumer orientated bodies to act as the front end for complaints.

Greater emphasis for ISAs would instead rest upon enforcement. This role could be performed either directly or supported via third party proxies in specific sectors e.g. financial services or healthcare regulators. Such an approach would have the added benefit of streamlining the regulatory burden as those being regulated would only have to look to a single regulator. Suitable sanctions would need to be established for transgressions against the measures described above. A system of fines and punishments would need to be developed and publicised, using criteria relevant to the risk to which personal data was exposed. Particularly deliberate misuse should be punished by criminal sanctions to act as both a direct punishment and as a deterrent to others.

ISAs would also be expected to share information about transgressors and act more strategically, considering the impact of their actions on the outcomes outlined. They might share information about persistent breaches of privacy by organisations across borders. The recent OECD Recommendation on Cross Border Co-operation in the Enforcement of Laws Protecting Privacy may be seen as a model approach[107], as is the cross border sharing of information between Computer Emergency Response Teams regarding information security risks and threats.[108]

In any respect, ISAs must evolve from being focused upon process and legal checking, to a broader advisory and enforcement role. This will mean that their staffing requirements will include economists, behavioural scientists and sociologists as well as legal experts and those with practical experience of data protection and privacy issues in public and private contexts.

---

[107] OECD 2007 *OECD Recommendation on Cross Border Co-operation in the Enforcement of Laws Protecting Privacy* http://www.oecd.org/sti/privacycooperation

[108] For instance see the *European Task Force –Computer Security Incident Response Team* (TF-CSIRT) http://www.terena.org/activities/tf-csirt/

To achieve this evolution, ISAs may also need to organise more specifically to deal with harms, compared to current structures focused on either functions (e.g. marketing, legal counsel, communications) or processes (e.g. enforcement, guidance or outreach). Current state of the art thinking on how regulation can deal with risk, harm or adverse impacts of policy challenges illustrate that existing normal function or process orientated structures of organisations may be outmoded when dealing with complex or ambiguous problems such as privacy.[109] Instead, organisations may need to be able to dynamically bring together different functional or process orientated teams to tackle problems by creating tailored solutions to achieve Outcomes rather than relying upon process orientated outputs such as numbers of files held or numbers of website hits. In this way results may thus be described in impact terms e.g. increased trust in organisations as a result of more responsible use of personal data. However, we recognise the inherent challenges in doing so due to the complexity of interlocking factors and difficulty of linking cause to effect but point to modern public sector evaluation methods as evidence of the possibilities of linking outputs to broader outcomes.

Responsibility for those collecting or using personal data

Under such a proposed regulatory regime, greater responsibility would be placed on organisations using personal data to use that data in accordance with the General Principles outlined above. Organisations, public and private, would have to take the initiative in choosing the most appropriate tool for their particular circumstance in accordance with local requirements, and would be held responsible for their decision removing opportunity for "abdication of responsibility".[110] The use of the tools will likely support the governance of the majority of the uses of personal data. There will always be a small minority that do not comply, either for reasons of error or more systematic failure. Enforcement should therefore be targeted at these organisations. More responsibility must rest with those using personal data, to take responsibility for their organisations and select which instruments are most relevant to their context and circumstance. In this way the market for personal data may become more self-managing, requiring less bureaucratic prior authorisations, checks and process orientated monitoring.

Responsibility for individuals / consumers

Making these new arrangements work would also empower individuals to take more responsibility for their own personal data. Naive exhortations to conduct 'awareness raising campaigns' must be replaced by a more sophisticated approach, using the tools above, to alert individuals to the consequences of their actions, educate them on the risk levels and provide them with the tools to take responsibility. Those providing these tools must recognise the complex psychological and mental factors, especially concerning the perceptions and attitudes toward risk that individuals have, for example negative discounting, the perception that it will 'never happen to me' and other mental models used

---

[109] See generally Sparrow, M. K. *The Character of Harms; Operational Challenges in Control* Cambridge University Press; Cambridge 2008

[110] Ayres, I. and Braithwaite, J. *Responsive Regulation; Transcending the De-regulation Debate*; Oxford Socio-legal studies; Oxford University Press; Oxford; 1992 p113

by individuals when deciding how to trade off their personal information for an expected social or economic benefit.

Finally, individuals must have a better appreciation of the consequences of their behaviour – however risky or not this might be. Whilst the right to privacy should be retained, there will invariably be consequences to exercising this right – and individuals must understand and be prepared to accept those consequences.

Recommendation 9 – Creation of a roadmap to achievement

Our final recommendation, following on from the Consultation, is that a roadmap to achieving this regulatory architecture should be developed. This may be an output from the regular European or International Conference of Data Protection and Privacy Commissioners. A first stage would be to conduct a substantive mapping exercise to determine what specific changes would need to take place in both national and European law, in order to bring about the regulatory architecture presented above. The role of the European Commission as Guardian of the Treaties would need to be considered carefully in any exercise.

4.4 Conclusion

The evidence gathered during this study showed clearly that the success or failure of privacy and data protection is not governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work.

The stronger, results oriented approach described in this report aims to protect data subjects against personal harm resulting from the unlawful processing of any data, rather than making personal data the building block of data protection regulations. It would move away from a regulatory framework that measures the adequacy of data processing by measuring compliance with certain formalities, towards a framework that instead requires certain fundamental principles to be respected, and has the ability, legal authority and conviction to impose harsh sanctions when these principles are violated.

REFERENCES

Reference List

2001 Future Bottlenecks in the Information Society Report, Institute for Prospective Technological Studies; see: http://ftp.jrc.es/EURdoc/eur19917en.pdf [accessed on April 1st 2009].

2004 Annual report from the Belgian Privacy Commission; see http://www.privacycommission.be/nl/static/pdf/annual-reports/verslag_over_de_werkzaamheden_2004.pdf [accessed on April 1st 2009].

2004 Declaration of the Article 29 Working Party (Working Party document WP 101) on Enforcement; see: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp101_en.pdf [accessed on April 1st 2009].

2005 Annual report from the Belgian Privacy Commission; see http://www.privacycommission.be/nl/static/pdf/annual-reports/verslag_over_de_werkzaamheden_2005.pdf [accessed on April 1st 2009].

2005 Economic Evaluation of the Data Protection Directive 95/46/EC; see http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf [accessed on April 1st 2009].

2006 Annual report from the Belgian Privacy Commission; see http://www.privacycommission.be/nl/static/pdf/annual-reports/verslag_over_de_werkzaamheden_2006.pdf [accessed on April 1st 2009].

Abrams., M., M. Crompton, and C. Cowper, *A possible way forward: Some themes and an Initial Proposal for a privacy and Trust Framework*, Privacy and Trust Partnership, November 2007.

Acoca, B., *Scoping Paper on Online Identity Theft, DSTI/CP(2007)3/FINAL*, Paris, France: Organisation for Economic Cooperation and Development, 2007, p. 6.

Acquisti, A., *Privacy in Electronic Commerce and the Economics of Immediate Gratification. Proceedings of ACM Electronic Commerce Conference (EC 04),* New York, USA: ACM Press, 2004, pp. 21-29.

Acquisti, A., *The Economics of Privacy – Resources on Financial Privacy, economics, anonymity*, 2005; see: www.heinz.cmu.edu/~acquisti/economics-privacy.htm [accessed on April 1st 2009].

Acquisti, A., S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati (eds), *Digital Privacy: Theories, Technologies and Practices*, Auerbach Publications, 2007.

Akçura, M.T. and K. Srinivasan, "Research Note: Customer Intimacy and Cross-Selling Strategy", *Management Science, Vol. 51, No. 6*, 2005, pp. 1007–1012.

Akerlof, G. A., "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics, Vol. 84, No. 3*, 1970, pp. 488-500.

Anderson, S.P. and A. de Palma, "A Theory of Information Overload", Toulouse, France: Institut d'Economie Industrielle, 2005; see: http://idei.fr/doc/conf/sic/papers_2005/sanderson.pdf, pp.1-31[accessed on April 1st 2009].

Anderson,S. P.., R. Clayton, and T. Moore, 2008, *Security Economics and the Internal Market,* paper prepared for the European Network Information Security Agency, 2008; see: http://enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf [accessed on April 1st 2009].

Art. 29 WP Working Document - Privacy on the Internet- An integrated EU Approach to On-line Data Protection (WP37 - 5063/00/EN/FINAL); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf [accessed on April 1st 2009].

Art. 29 WP Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union (WP43 - 5020/01/EN/Final); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf [accessed on April 1st 2009].

Art. 29 WP Sixth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries - covering the year 2001, 2003; see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/2003-6th-annualreport_en.pdf [accessed on April 1st 2009].

Art. 29 WP Seventh Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries - covering the years 2002 and 2003, 2004; see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/7th_report_prot_individs_en.pdf [accessed on April 1st 2009].

Art. 29 WP Declaration of the Article 29 Working Party on Enforcement (WP101 - 12067/04/EN); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp101_en.pdf [accessed on April 1st 2009].

Art. 29 WP Opinion on More Harmonised Information Provisions, and Annexes (WP100 - 11987/04/EN); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf and http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100a_en.pdf [accessed on April 1st 2009].

Art. 29 WP Opinion on More Harmonised Information Provisions, and Annexes (WP100 - 11987/04/EN); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf [accessed on April 1st 2009].

Art. 29 WP Eighth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2004, 2005; see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/8th_annual_report_en.pdf [accessed on April 1st 2009].

Article 29 WP report 106 on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union, adopted on 18 January 2005; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf

Art. 29 WP 9th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2005, 2006; see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/9th_annual_report_en.pdf [accessed on April 1st 2009].

Art. 29 WP Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive (WP126 - 1611/06/EN); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf [accessed on April 1st 2009].

Art. 29 WP 10th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2006, 2007, see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/10th_annual_report_en.pdf [accessed on April 1st 2009].

Art. 29 WP Opinion Nº 4/2007 on the concept of personal data (WP136 - 01248/07/EN); see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf [accessed on April 1st 2009].

Ayres, I. and Braithwaite, J. *Responsive Regulation; Transcending the De-regulation Debate*; Oxford Socio-legal studies; Oxford University Press; Oxford; 1992

Bennett C. J., and C. Raab, *The Governance of Privacy: policy instruments in a global perspective*; 2nd Edition, London, UK: MIT Press, 2006, p. 97.

Blick, A, and S. Weir, *The Rules of the Game: The Governments counter-terrorism laws and strategy: A Democratic Audit Scoping Report* York, UK: Joseph Rowntree Reform Trust, November 2005.

Buchta, A., "PRIME Legal Requirements Version 0 - Part 1", Prime Project, 2004; see https://www.prime-

project.eu/prime_products/reports/reqs/pub_del_D01.1.a.part1_ec_wp01.1_V2_final.pdf [accessed on April 1st 2009].

Camenisch, J., A. Shelat, D. Sommer, S. Fischer-Hübner, M. Hansen, H. Krasemann, G. Lacoste, R. Leenes, J. Tseng, *Privacy and Identity Management for Everyone*, PRIME Project; see http://www.zurich.ibm.com/%7Ejca/papers/cssf05.pdf [accessed on April 1st 2009].

Cappato, M., "Report on the First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)", Brussels, Belgium: European Commission; see: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/ep_report_cappato_04_en.pdf [accessed on April 1st 2009].

Carroll, K., and D. Coates, "Teaching Price Discrimination: Some Clarification", *Southern Economic Journal, Vol.66, No.2*, 1999, pp. 466-480.

Cave, J., C. Marsden, and S. Simmons, *Options for and Effectiveness of Internet Self- and Co-Regulation* Santa Monica, USA: RAND, TR-566-EC, 2008.

Chang, H.-J., " The Market, the State and Institutions in Economic Development", in Chang, H.-J. (ed.), *Rethinking Development Economics*, London: Anthem Press, 2003, pp. 41-60.

Chellappa, R.K., and S. Shivendu, "An Economic Model of Privacy: A Property Rights Approach to Consumer Concerns of Privacy in Online Personalization: Incentives and Welfare Implications", 2003; see: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=457003, pp. 1-38 [accessed on April 1st 2009].

Coase, R.H., "The Problem of Social Cost", *Journal of Law and Economics, Vol.3*, 1960, pp. 1-44.

Cohen, J.E., "Examined Lives: Informational Privacy and the Subject as Object", Stanford Law Review, Vol. 52, No.5, 2000, pp.1373-1438.

Coleman, J.S., "An Introduction to Privacy in Economics and Politics: A Comment", *The Journal of Legal Studies, Vol. 9, no. 4*, 1980, pp. 645- 648.

Commission Nationale de l'Informatique et des Libertés, *2008 Annual Report of the Commission Nationale de l'Informatique et des Libertés*, Chapter 1 "Measuring Diversity: Ten Recommendations", Paris, France: Commission Nationale de l'Informatique et des Libertés, 2008.

Crossman, G., H. Kitchin, R. Kuna, M. Skrein, and J. Russell, *Overlooked: Surveillance and personal privacy in Modern Britain Liberty*, London, UK: The Nuffield Foundation, October 2007.

Culnan, M.J., R. J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations", *Journal of Social Issues, Vol.59, No.2*, 2003, pp. 323-342,

Dodds, S. "Privacy and Endogenous Monitoring Choice When Private Information is a Public Good", 2003; see:

http://www.econ.queensu.ca/working_papers/papers/qed_wp_1010.pdf [accessed on April 1st 2009].

Easterbrook, F.H. "Privacy and the Optimal Extent of Disclosure under the Freedom of Information Act", *The Journal of Legal Studies, Vol. 9, No. 4*, 1980, pp. 775-800.

European Commission, First Report on the transposition of the Data Protection Directive, 2003; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT [accessed on April 1st 2009].

European Commission, "Working Party document WP 100 - Opinion on more harmonised information provisions" adopted, Brussels, Belgium: European Commission, 2004; see: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf [April 1st 2009].

European Commission, "Working Party document WP 106 - Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union", Brussels, Belgium: European Commission, 2005; see: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf [accessed on April 1st 2009].

European Commission, Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive, March 2007; see http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf [accessed on April 1st 2009].

European Data Protection Supervisor (EDPS), *2004 Annual Report*; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2004/Annual_Report_2004_EN.pdf [accessed on April 1st 2009].

European Data Protection Supervisor (EDPS), *2005 Annual Report;* see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2005/AR_2005_EN.pdf [accessed on April 1st 2009].

European Data Protection Supervisor (EDPS), *Background paper on Public access to documents and data protection*, 2005; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/05-07_BP_accesstodocuments_EN.pdf [accessed on April 1st 2009].

European Data Protection Supervisor (EDPS), *2006 Annual Report*; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2006/AR_2006_EN.pdf [accessed on April 1st 2009].

European Data Protection Supervisor (EDPS), *2007 Annual Report*, see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2007/AR2007_EN.pdf [accessed on April 1st 2009].

European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection* Brussels, Belgium: EDPS, November 2008; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf [accessed on April 1st 2009].

European Network and Information Security Agency (ENISA), "Security Issues and Recommendations for Online Social Networks", *Position Paper, No. 1,* October 2007; see: http://enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf [accessed on April 1st 2009].

Future of Identity in the Information Society (FIDIS), "D13.3: Study on ID number policies", 2007; see: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp13-del13_3_number_policies_final.pdf [accessed on April 1st 2009].

Future of Identity in the Information Society (FIDIS), "D13.6 Privacy modelling and identity", 2007; see: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp13-del13.6_Privacy_modelling_and_identity.pdf [accessed on April 1st 2009].

Future of Identity in the Information Society (FIDIS), "D14.2: Study on Privacy in Business Processes by Identity Management", 2007; see: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp14-del14.2-study_on_privacy_in_business_processes_by_identity_management.pdf [accessed on April 1st 2009].

Future of Identity in the Information Society (FIDIS), "D14.3: Study on the Suitability of Trusted Computing to support Privacy in Business Processes", 2007, see http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp14-del14.3_Study_on_the_Suitability_of_Trusted_Computing_to_support_Privacy_in_Business_Processes.pdf [accessed on April 1st 2009].

Future of Identity in the Information Society (FIDIS), "D5.2b: ID-Related Crime: Towards a Common Ground for Interdisciplinary Research", 2005; see: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf [accessed on April 1st 2009].

Financial Services Authority (FSA), "Decision Procedure and Penalties Manual Release 070 Section 6.2", October 2007: see: http://www.fsa.gov.uk/pubs/hb-releases/rel70/rel70depp.pdf [accessed on April 1st 2009].

Hann, I.-H., K. L. Hui, T. S. Lee, and I.P.L. Png, "Consumer Privacy and Marketing Avoidance", 2005; see@ http://www-rcf.usc.edu/~hann/publications_files/consumer_privacy_and_marketing_avoidance.pdf [accessed April 1st 2009].

Hart, O.D. and J. Tirole, "Contract Renegotiation and Coasian Dynamics", *The Review of Economic Studies, Vol. 55, No. 4*, 1988, pp., 509 – 540,

Hermalin, B.E. and M. L. Katz, "Privacy, Property Rights & Efficiency: The Economics of Privacy as Secrecy", *Quantitative Marketing and Economics, Vol. 4, No. 3.,* 2006.

Hirshleifer, J., "The Private and Social Value of Information and the Reward Incentive to Activity", *The American Economic Review, Vol. 61, No. 4*, 1971, pp. 561-574.

Hoven, Jvd., "Information Technology, Privacy and the Protection of Personal Data", in Weckert, J., and Jvd. Hoven (eds), *Information Technology and Moral Philosophy* Cambridge, UK: Cambridge University Press, 2008, p. 311.

Hui, K.-L. and I.P.L. Png, "The Economics of Privacy", 2005; see: http://129.3.20.41/eps/io/papers/0505/0505007.pdf [accessed on April 1st 2009].

Hustinx, P., "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive: Opinions of the European Data Protection Supervisor", *Official Journal of the European Union C 255*, October 2007, p. 2; see: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf [accessed on April 1st 2009].

Hustinx, P., *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection* Brussels, Belgium: European Data Protection Supervisor, November 2008.

Jones, A., B. Sufrin and B. Smith, B. *EC Competition Law: Text Cases and Materials* Oxford University Press Oxford 2007

Joseph, G. W., L. N. Bostick, and L. T. Slaughter Jr, "Web Assurance Seals – Are they All Alike? A look at web-trust and other Web Assurance Seals", *Journal of the International Academy for Case Studies, Vol. 11 No. 4*, 2005.

Kakalik, J. S., T. Dunworth, T., L. A. Hill L. A., et al., *An Evaluation of Mediation and Early Neutral Evaluation Under the Civil Justice Reform Act,* Santa Monica, USA: RAND, 1996, MR-803.

Korff, D., "EC Study on the Implementation of the Data Protection Directive - comparative summary of national laws", Colchester, UK: University of Essex Human Rights Centre, 2002; see: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf [accessed on April 1st 2009].

Lace, S. (ed), *The Glass Consumer: Life in a Surveillance Society*, London, UK: National Consumer Council, 2006.

Laudon, K.C., "Markets and Privacy", *Communications of the ACM, Vol.39, No.9*, 1996, pp. 92-104.

Leenes, R., J. Schallaböck, and M. Hansen, "PRIME White Paper Version 3", Prime Project, 2008; see https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf [accessed on April 1st 2009].

Leith, P. "Squeezing Information out of the Information Commissioner: Mapping and measuring through online public registers", *SCRIPTED 389, Vol. 3, No. 4, 2006*; see:

http://www.law.ed.ac.uk/ahrc/script%2Ded/vol3-4/leith.asp [accessed on April 1st 2009].

Marcus, J. C., K. Carter, N. Robinson, L. Klautzer, C. Marsden, et al., "*Comparison of Privacy and Trust Policies in the Area of Electronic Communications - Final Report*", Brussels, Belgium: European Commission, 2007; see: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_20_07_07_pdf.pdf, p. 10 [accessed on April 1st 2009].

Margulis, S.T., "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues, Vol. 59, No. 2*, 2003, pp. 243-261.

McDonald, A.M., and L. F. Cranor, *The Cost of Reading Privacy Policies,* Preprint for Telecommunications Policy Research Conference, November 2008.

Ministry of Justice UK, "The 2002 Proposals for Amendment of the Data Protection Directive (95/46/EC), made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note", 2002; see: http://www.dca.gov.uk/ccpd/dpdamend.htm [accessed on April 1st 2009].

Office of the Privacy Commissioner of Canada, *Assessing the Privacy Impact of Programs Plans and Policies,* 2007; see: http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf [accessed on April 1st 2009].

O'Harrow, R. Jr., "Night and Day, Computers Collect Information", *Washington Post*, Wednesday May 16 2001; see: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=washtech/techweek&contentId=A26622-2001May14, p. G10 [accessed on April 1st 2009].

Organisation for Economic Cooperation and Development, "The Seoul Declaration for the Future of the Internet Economy", Paris, France: OECD, 2008; see: http://www.oecd.org/dataoecd/49/28/40839436.pdf [accessed on April 1st 2009].

Perri, 6, "Whats in a frame? Social Organisation, Risk Perception and the sociology of knowledge", *Journal of Risk Research, Vol. 8. No. 2,* 2003, pp. 91–118.

Pfitzmann, A., and M. Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology (v0.31)*, 2008; see http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf [accessed on April 1st 2009].

Posner, R. A., "The Economics of Privacy", *The American Economic Review, Vol.71, No.2*, 1980, pp. 405-409.

Privacy in Research Ethics and Law (PRIVIREAL), "Recommendations from PRIVIREAL to the European Commission", 2005; see: http://www.privireal.org/content/recommendations [accessed on April 1st 2009].

Raab, C.D., "From Balancing to Steering: New Directions for Data Protection" in C. J. Bennett and R. Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age*, Toronto, Canada: University of Toronto Press, 1999, pp. 68-95.

Rule, J., and L. Hunter, "Towards Property Rights in Personal Data", in C. J. Bennett and R. Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age*, Toronto: Canada, University of Toronto Press, 1999, pp. 168-181.

Solove, D.J., *Understanding Privacy* Cambridge, USA: Harvard University Press, 2008, p. 196.

Sparrow, M. K. *The Character of Harms; Operational Challenges in Control* Cambridge University Press; Cambridge 2008

Stigler, G.J., "An Introduction to Privacy in Economics and Politics", *The Journal of Legal Studies, Vol. 9, no. 4*, 1980, pp. 623-644.

Taylor, C.R., "Consumer Privacy and the market for customer information", *RAND Journal of Economics, Vol. 35, No. 4*, 2004, pp. 631-650.

Thaler, R. H., and C. R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* New Haven, USA: Yale University Press, 2008, p. 34.

Van de Voort, M., and A. Ligtvoet, "Towards and RFID policy for Europe: Workshop Report", Leiden, The Netherlands: RAND Europe, DRR-4046-EC, 2006; see: http://www.rfidconsultation.eu/docs/ficheiros/RFID_Workshop_Reports_Final.pdf [accessed on April 1st 2009].

Walport, M., and R. Thomas, *Data Sharing Review*, London, UK: Her Majesty's Stationary Office (HMSO), 2008.

Warren, S.D., and L. D. Brandeis, "The Right to Privacy", *Harvard Law Review, Vol. 4 No. 5*, 1890.

West, R., "The psychology of security: why do good users make bad decisions?" *Communications of the ACM* Vol. 51, No. 4, 2008, pp. 34-40.

Westin, A., *Privacy and Freedom* New York, USA: Atheneum, 1967.

Wilde, G.J.S., *Target Risk 2: A New Psychology of Safety and Health*, Toronto, Canada: PDE Publications, 2001.

Winer, R.S., "A framework for Customer Relationship Management", *California Management Review, Vol. 43, No. 4*, 2001, pp. 89–105.

APPENDICES

Appendix A: Research Methodology

In conducting this study, we utilised a number of research approaches specifically tailored to each phase. Both the literature review, web survey and the interviews were used to understand the current state of the art regarding the use of personal information and the strengths and weaknesses of the Directive. These exercises then fed into a scenario based workshop toward the end of the study. The purpose of the interview based evidence gathering was thus not to conduct a widespread consultation or definitive identification of the issues, but rather to confirm understanding of our analysis of the issues arising from the literature review, solicit ideas for ideas for improvement and update knowledge.

- **Desk Research**

We reviewed the literature from a number of domains, including the law itself (both the Directive and applicable national law), Opinions and commentary of the Article 29 Working Party and European Data Protection Supervisor and annual reports of Data Protection Authorities were also consulted. We also reviewed articles, papers, reports and other material from the legal literature regarding the perceived strengths and weaknesses of the Directive. We also reviewed literature from the emergent fields of the economics of privacy and information security, behavioural economics, sociology and regulatory approaches and European policy-making. We also reviewed and considered different approaches to privacy protection, ranging from the Organisation for Economic Co-operation and Development to Asia Pacific Economic Co-operation efforts and regimes in North America and Australasia.

- **Semi Structured Interviews**

We conducted around 50 semi-structured interviews on a non-attributable 'Chatham House rule' basis. Interviewees are listed at the end of this report. These interviewees ranged from representatives of independent supervisory authorities, policy-makers and officials to privacy professionals from various industry sectors, consumer organisations and finally academics and established experts. Interviewees were deliberately global in nature and we attended the International Conference of Data Protection Commissioners in Strasbourg which gave us further opportunity to conduct face to face interviews with stakeholders from across the globe. A small number of telephone interviews were conducted when it was not practicable to conduct face to face interviewees. In order to supplement the interviews, we also opened a short online survey instrument. This was open from August 2008 to November 2008 and had 5 responses. Invitations were mailed to an unbounded sample size of contacts and interested experts in the area of privacy and data protection.

- **Scenario based workshop**

On 28th November 2008 the ICO hosted a scenario based workshop in London which represented the final element of our study methodology. We invited a broad range of privacy and data protection stakeholders, including some representatives from European and international independent supervisory authorities, and Data Protection Commissioners, data protection and privacy professionals from a range of industry sectors, & noted experts and academics. The workshop had 23 attendees plus representatives from the Information Commissioners Office and the study team. A scenario based methodology was used to identify key uncertainties of possible futures and review how the Directive would stand up against them. Participants were asked to consider what changes would need to be made now in order to ensure insofar as possible the Directive remained valid in the face of these future uncertainties. The discussion at the workshop remained at a high level, staying away (consistent with the remit of the study) from detailed legalistic interpretation of the Directive's text.

Appendix B: List of Interviewees

Alain Brun (European Commission, DG Justice, Freedom and Security)

Alessandro Acquisti (Expert)

Alexander Dix (Commissioner for Data Protection and Freedom of Information, State of Berlin, Germany)

Anne Carblanc (Organisation for Economic Co-operation and Development)

Anna Fielder (Consumer Focus)

Blair Stewart (Office of the Privacy Commissioner, New Zealand)

Bojana Bellamy (Accenture)

Carsten Casper (Gartner Group)

Caspar Bowden (Microsoft EMEA)

Charles Raab (Expert)

Chris Kelly (Facebook)

Christopher Kuner (European Privacy Officers Forum and Hunton and Williams)

David Trower (IMS Health EMEA)

Dirk van Rooij (European Commission DG Information Society and Media)

Dominique Pissoort (Belgian Direct Marketing Association)

Dorothy Patton (Consultant)

Francis Aldhouse (Bird and Bird LLP)

Francesco Pizzetti (Garante per la protezione dei dati personali, Italy)

Gerald Deprez (European Parliament)

Jacob Kohnstamm (Dutch Data Protection Authority, Netherlands)

Jannine Aston (Verizon Business EMEA)

Jennifer Barrett (Acxiom)

Jennifer Stoddart (Canadian Privacy Commissioner, Canada)

Jeremy Ward (Symantec)

Jeremy Beale (Confederation of British Industry)

John Kropf (Department of Homeland Security, United States)

Kamlesh Bajaj (Data Security Council of India)

Karen Curtis (Office of the Privacy Commissioner, Australia)

Katrine Evans (Office of the Privacy Commissioner, New Zealand)

Luc Van Assche (Belgian Direct Marketing Association)

Malcolm Crompton (Information Integrity Solutions Pty Ltd)

Marie Shroff (Office of the Privacy Commissioner, New Zealand)

Martin Abrams (Hunton & Williams)

Martin Hoskins (T-Mobile (UK) Ltd)

Marta Ayed (Confianza Online)

Melanie Shillito (British Banking Association)

Michael Donahue (Organisation for Economic Co-operation and Development)

Nathalie Lambert (IMS Health, France)

Neil Matthews (Acxiom Ltd)

Nick Tyler (Astra Zeneca)

Peter Church (Linklaters)

Peter Cullen (Microsoft)

Peter Hustinx (European Data Protection Supervisor)

Peter Schaar (The Federal Commissioner for Data Protection, Germany)

Richard Boase (British Banking Association)

Richard Clumbley (Linklaters)

Roderick Woo (Office of the Privacy Commissioner, Hong Kong Special Administrative Region)

Ruth Boardman (Bird and Bird)

Sue Gold (The Walt Disney Company Limited)

Ulrike Dellrud (Expert)

Yael Weinman (Federal Trade Commission, United States)

Appendix C: Workshop Terms of Reference & Scenario Framework

The UK Information Commissioner's Office (ICO) has commissioned a review into the EU Data Protection Directive 95/46/EC, specifically into its strengths and weaknesses and to explore potential avenues for improvement of its application.

This review addresses concerns that certain provisions of the Directive may no longer optimally serve their purpose of protecting individuals against abuses of their personal information and supporting the free flow of this information in the internal market. These concerns are especially acute given technical and societal changes that seem to increasingly favour the facilitated and extended use of personal information.

The study considers a number of issues arising from the practical application of the Directive and its impact. It does this by reviewing the broad canon of research available in this domain, enhanced by interviews with key stakeholders.

Based on the information collected the study team is now organising a scenario based workshop, hosted by the UK Information Commissioner in London.

We're looking forward to welcoming you to this workshop. We want to work with you to explore the challenges that lie ahead in the area of data protection and privacy, and to consider how best to tackle them. This letter will give you a first idea of what will happen at the workshop. You don't need to do anything in preparation, except show up with an open mind, and your own knowledge and experience!

Your workshop team,

Neil Robinson	Hans Graux	Maarten Botterman
RAND Europe	time.lex	GNKS Consult

Focus areas for discussions

Our research and interviews with experts demonstrated that a few similar issues arise, time and time again. These are the main subjects that we intend to tackle.

Dealing with technological and societal changes

When the European Data Protection Directive was initially drafted, the world was very different from today. The enormous richness of data, particularly on-line, has increased beyond comprehension since the time of the Directive's creation. The improved capacity to collect and handle personal data, wherever and whenever, has offered many different opportunities, both at the micro-level – personalising individual services – and at the macro level - using profiling to support strategic decision making. While the Directive's framework was intended to be technology-neutral, implementations and interpretations can sometimes be more restrictive when it comes to new uses of personal data. And in the information society, change can go far beyond what one could reasonably imagine more than a decade ago. In this environment, it may not be sufficient to simply adapt the framework to today's realities: maybe it is time to support the procedural aspects of the Directive with consideration of harm-based punishment, as no prescriptive provision would be able to deal with the unforeseen use of new technologies and applications.

Complying with rules in a globalised society

While the Directive was adopted by all Member States, the way legislation is set up and interpreted varies a lot between Member States. The good news is that this leads to a myriad of experience. This diversity can lead to solutions that have a positive impact on our ability to protect data and privacy. The bad news is that the consistent protection of people from abuse of their personal data across borders is not always easy, or even possible. Outside the European context, companies that trade internationally are confronted with different rules in different jurisdictions, and often need to adapt their policies and practices, which can lead to high transaction costs. Currently those issues are addressed in different ways, none of them entirely satisfactorily. Self-regulation is sometimes seen as an answer to this issue; however, this would require clearer legal authority for such an initiative which currently does not exist under European rules.

Stimulating investment in protection of privacy

All things considered, businesses today often have no incentive to invest in privacy protection measures. There is no clear universal perception of a "gold standard" of data protection, and good privacy practices are not yet recognised as a competitive advantage by consumers until a "privacy disaster" is widely published. Businesses claim they would be more eager to comply with data protection rules if compliance was made easier, less costly, and not burdened with sometimes contradictory legislation or unrealistic expectations from the regulators. Other contributing factors which do not help to embed good data protection practice include differences in rules (e.g. regarding enforcement) between countries that help to create a perception of data protection simply as a barrier and administrative formality.

Trends and uncertainties

We will explore these and other issues with you in the light of six global trends that will affect the way our world looks in 2020.

1. Globalisation trends: Universal connectivity and access, and the cost and benefits of diversity;
2. People trends: how technology is used in new ways is being led by our kids, and the empowerment of the individual;
3. Technology trends: a new era of pervasive computing, creating intelligent environments;
4. Relevant security trends: Accepting risks, increasing transparency and taking precautions just like in the physical world;
5. Relevant economic trends: Balancing collaboration and competition, stability and innovation;
6. Governance trends: accepting the global, multi-faceted nature of the Internet and dealing with failing jurisdictions and poor enforcement.

These trends are very likely to develop further, but how they will ultimately work out is uncertain. We will consider the likelihood of these trends as well as the impact they might have on requirements for data protection and privacy.

Major uncertainties that will result from different choices in our future may also have a high impact. Here we will consider:

- Technological progress: will the world continue to move towards more high-tech, connected environments and rich communications across platforms, or can we expect a certain break-down of connectivity and interoperability at some point?
- Ability of "the on-line environment" to identify and authenticate actors on-line, and to provide information security and data protection. For true privacy protection we need to be able to make sure only those who legitimately have access to certain (levels of) information have it. This needs to be backed by robust information security measures and use of privacy enhancing methods and technologies. Will this be adequate by 2020, or are we still in the dark?
- Appreciation of privacy: will our needs for protection of privacy through legislative frameworks still exist, or will we have learned different ways of dealing with it, and is protection needed on a different level? We only need to watch our children play to understand that "we don't really know";
- Harmonisation and collaboration in protection across jurisdictions. Will this have improved in ten years time? What efforts will be needed to protect us in a world in which data are borderless?

Scenario story

The scenario story, a picture of the future, is 'a coat hanger' for the discussion. This scenario story will be internally consistent, plausible, engaging and fun. All elements that determine that future (the major certainties and uncertainties) will be reflected in this

picture of the future. We will then test how the impact of these uncertainties changes depending upon where we might end up.

Tasking

Once we have presented the scenario story, we will discuss with you:

1. In what way you see the different dimensions working out, what you like/dislike overall, and what threats and opportunities you see in that future (SWOT)?
2. What are the positive and negative ends for the key dimensions that matter most, and what influences the occurrence of those and determines the future?
3. Knowing this, what actions should have been taken in the near future to get the best possible outcome?

By following this approach, there is one compelling story that is set up to consider multiple dimensions. The discussion will thus touch upon all dimensions and focus on those that seem to have the most impact. In this way, without predetermined extremes, the moderated discussion will allow the knowledge and experience of all participants to truly unfold.

Agenda for the meeting

09:30	Welcome by the Information Commissioner
09:45	Introduction of the participants to the debate (what did we learn from literature and interviews), and explanation of the "rules of the game"
10:15	Introduction of the scenario story, and initial set of relevant dimensions
10:45	Coffee break
11:00	SWOT analysis of the Directive against the scenario story
12:00	Lunch
13:00	Discussion on the relevant dimensions, followed by prioritisation and selection of dimensions to be further explored, and exploration of selected key dimensions
14:00	SWOT analysis of the Directive taking into account possible extremes in key dimensions
15:00	Tea break
15:15	Having explored all this, what needs to be done TODAY in order to ensure the best possible data and privacy protection towards the future
16:00	Preliminary conclusions by the Project Team
16:15	Closure by Information Commissioner

Appendix D: Policy conclusions from the workshop

In the 3rd session we asked the question what needs to be done today in order to ensure the best possible data and privacy protection toward the future

Summary: 5 Key Findings

Future Data Protection measures must:

1) Focus on misuse of data (back-end 'harm')
2) Overcome difficulties associated with implementation
3) Use framework of "BCRs"
    a. Minimal standards requirements
    b. Obligation to have a privacy policy
4) Incorporate a liability framework and sanctions
    a. For harm-
    b. For breaches of declarations on, say, BCRs
5) Overcome conflicting laws

Summary Table of Roundtable Contributions by Topic

Issue	Summary
Awareness	Awareness of the issues of Data Protection and privacy should be increased.
Balancing Needs	Needs of consumers, businesses and government must be balanced.
Clarity	Any measures need to be clear, appropriately focused and implementable.
Consent	Role of consent depends on societal factors and the ability of public to make informed decisions on privacy.
Definition and degrees of 'personal information' and 'sensitive data'	Some data is more personal than others; 'sensitive' is a subjective term.
External Enforcement Organisation vs. Internal Compliance Mechanisms	Opinion divided on whether an external body must drive process or whether internal corporate structures should be harnessed to improve data protection measures.

Harm	Consensus that harm is a difficult concept to operationalise in this context. More appropriate to discuss 'risk' or harm in a back-end framework.
Harmonisation and Global Context	Harmonisation was urged; European approach too narrow given outsourcing practices etc.
Privacy vs. Data Protection	Potential disparity in Data Protection and privacy measures – DP is a practical legal issue whereas privacy is a civil liberties/human rights issue.
Public Vs. Private Sector	Measures proposed for private sector (e.g. BCRs) might not be appropriate in a public sector context etc.
Responsibility and Accountability	Often unclear where responsibility lies and who is accountable, especially in situations where a person's personal data can impact upon the privacy of others.
Sanctions	Sanctions regimes deemed appropriate where promises made by companies are not fulfilled (e.g. BCRs); but must be large enough to offer a significant disincentive.
Scope and Jurisdiction	Clarity required on where jurisdiction lies and what the scope of any directive is. Issue clouded by cross-border flows, multinational corporations, outsourcing practises, cookies etc.
Technology	No consensus on role of technology in future data protection measures. Some thought it could be harnessed to improve systems; others argued it is no substitute for appropriate human processes

Appendix E: List of workshop attendees

Richard	Thomas	UK ICO
Iain	Bourne	UK ICO
Emma	Butler	UK ICO
Jonathan	Cave	RAND Europe
Jos	Dumortier	Timelex
Lorenzo	Valeri	RAND Europe
Neil	Robinson	RAND Europe
Maarten	Botterman	GNKS-Consult
Hans	Graux	Timelex
Greg	Falconer	RAND Europe
Rhian	Hill	Bird and Bird
Martin	Hoskins	T-Mobile UK
Nick	Tyler	AstraZeneca
James	Barker	Hewitt
Bojana	Bellamy	Accenture
Dilip	Amin	National Police Improvement Agency
Peter	Sommer	London School of Economics
Melanie	Shillito	British Banking Association
Charles	Raab	University of Edinburgh
Marco	Cassata Mont	HP Labs
Marta	Ayed	Confianza Online
Anne-Marije	Fontein-Bijnsdorp	Dutch Data Protection Authority
Dorothy	Patton	Consultant
Samoera	Jacobs	FEDICT
Neil	Matthews	Axicom
Sue	Gold	Disney