The European perspective - is Data Protection value for money?

Dr. Peter R. Harris

Data Protection Commissioner, Bailiwick of Guernsey
P.O. Box 642, St. Peter Port, Guernsey, Channel Islands GY1 3JE
dataprotection@gov.gg

Abstract
This paper aims to examine the economics of the regulation of the processing of personal data in the context of the 1995 European Directive on Data Protection. The major elements of the Directive and their impact on costs are identified and quantified where possible. Reference is made to published assessments of cost published by the UK Government in 1997 and 2003 and to the expenditure of the Commissioners in the UK and Ireland. These are compared and contrasted with a number of mostly intangible benefits associated with the relatively strong regulatory environment that results from implementation of the Directive. The question is raised as to whether the costs of strong regulation are justified by the economic benefits that ensue.

1. Introduction

Both business and government exploit Information and Communications Technologies to obtain process efficiency, and aim to maximise the use of information sharing to combat fraud and to provide tailored personalised services to individual customers.
Free market economics relies on competition to drive down prices, but needs adequate regulation to ensure fairness of trading and consumer protection.
The regulation of the processing of personal data interferes in the free market by enforcing individuals' rights and imposing standards of processing on organisations, so it is perhaps not surprising that anyone who regulates personal data processing may be required to provide an economic justification for their existence.
Regulation is also required of the public sector's use of technology to ensure that human rights are not compromised by the unwarranted sharing or unnecessary publication of personal information by government.
In Europe, regulation has tended to develop on the basis of statutory powers vested in independent public officials, whereas elsewhere in the world there may have been a greater tendency to encourage self-regulation.
There appears to be a generally held belief that Data Protection is a "good thing", but very little evidence as to whether the costs of compliance are balanced by the overall economic benefits to society.

1.1. OECD

The Organisation for Economic Co-operation and Development was established to promote policies designed to encourage economic development and a rising standard of living on a multilateral, non-discriminatory and global basis.
The Recommendation concerning the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[1] was adopted by the Council of the OECD on 23rd September 1980.
This document was designed to stimulate international trade by defining eight principles of good practice that should apply to the protection of privacy.
Broad political attention was first given to privacy online at the OECD Conference "Dismantling the Barriers to Global Electronic Commerce" held in Turku, Finland, on 19-21 November 1997 and in the following year, the Ottawa Ministerial Declaration reaffirmed a " commitment to the protection of privacy

on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data".
Much of the work of the OECD in this area is detailed in: "*Privacy Online: OECD Guidance on Policy and Practice"* [2], and further information may be found on the OECD website[3]. In the privacy sphere, the OECD has sought to build bridges based on voluntary compliance with their recommendations rather than by establishing binding international treaties. However, it is evident that the members of the OECD believe that globally uniform standards of privacy protection would benefit international economic activity.

1.2. Council of Europe

At about the same time as the OECD was developing its eight principles, the regulation of Data Protection throughout Europe was being initiated by the publication of the 1981 Council of Europe Convention 108[4]; this came into force in 1985, has since been ratified by 31 Parties - including all the present EU Member States - and has also been signed by 7 other countries.
Convention 108 defined common minimum standards that were to be applied to the automated processing of personal data: it established the 5 principles of data quality, introduced the concept of special categories of data and established the rights of individuals in respect to information processed about them. Parties to the Convention were encouraged not to inhibit trans-border flow of personal data to another Party for reasons connected with privacy protection.
Some countries already had Data Protection legislation prior to Convention 108 and the subsequent implementation of national legislation in other countries diverged significantly between different European countries. The definitions of personal data were not consistent, some including manual records, for example, whilst others specifically excluded sound and image data. Some countries extended protection to legal persons, whilst others restricted protection to data about living individuals.
The result was that, despite the binding nature of the Convention, the flow of data between States was being impeded, owing to the different levels of protection in force and prohibitions by those with the strongest legislation from transfers to those States and territories with a lower standard of protection.

1.3. The Data Protection Directive

In the late 1980's, the economic consequences of the divergence of Data Protection standards were potentially quite acute and beginning to threaten the proper functioning of the Internal Market within the [then] European Economic Community. There was at least one instance, for example, where computerised personnel records of workers in one Member State were prevented from being transferred to the head office of the company that was established in another Member State. It was evident that the unequal protection of personal data was having an adverse effect on the economic progress on the Internal Market.
The European Commission responded to these by drafting a Data Protection Directive in 1990. This was not finally adopted until 1995[5] and imposed a common generally higher standard of protection and regulation across all Member States. The twin objectives of the Directive expressed in Article 1 were:

1. to protect the rights of individuals with respect to the processing of their personal data; and
2. to facilitate the free movement of personal data between Member States.

Although it was the first objective that received much attention, it was the second that held out the prospect of major economic benefit.
However, the economic benefits came at the costs of compliance with the more uniform, but higher, standards of the national legislation resulting from the Directive and it is worth asking whether the facilitation of trade within the European Union has come at the cost of inhibiting the development of trade with Third Countries.

2. Elements of Cost

Costs may be classified as tangible or intangible as shown in the table below:

TANGIBLE	INTANGIBLE
Supervisory Authority	Impact on competitiveness
Notification Fees	Limitation on sharing of data
Compliance	Excessive bureaucracy
Subject Access	

The tangible costs of Data Protection comprise two main elements:

a) The cost of running the supervisory authority and the payment of any fees for notification; and
b) Compliance with the Data Protection principles, in particular the costs of the provision of data subject access.

Intangibles include:

c) The perception that compliance might reduce competitiveness, by limiting what can be done with customers' information; and
d) Inefficiencies introduced by restrictions on the sharing of data and the additional bureaucracy associated with compliance activities.

The major elements of the Directive that are of particular relevance to this paper are:

1. compliance with the Data Protection principles,
2. respecting the rights of data subjects,
3. administration of the notification process,
4. controlling data transfer to third countries and
5. exercising the functions of the supervisory authority.

2.1. Compliance with the Principles

The costs of compliance are borne by both the public and private sectors. In the private sector all businesses need to have regard to the privacy rights of their staff, but the main element of cost is likely to be determined by the extent to which an organisation transacts business with private individuals and then whether these transactions involve the processing of sensitive personal data.

In January 1994, the UK Home Office undertook a survey about the economic impact of the Directive [that was at that time still in a draft form] on 625 organisations, drawn from central government, local government, charities, private sector organisations and trade associations. The conclusions of that initial study[6] were that set-up costs would amount to £2.24 billion (€3.34bn) and that annual expenditure on data protection would rise by a factor of 25 to £308 million (€460m). However, that estimate received some criticism (for example in Data Protection News[7]) and a report by Ashton Business School and the Universities of Tilburg and Leiden[8] found in 1994 that : *"The financial impact of the proposed Directive will be very small for the majority of organisations studied in the public and private sectors in the Netherlands."*

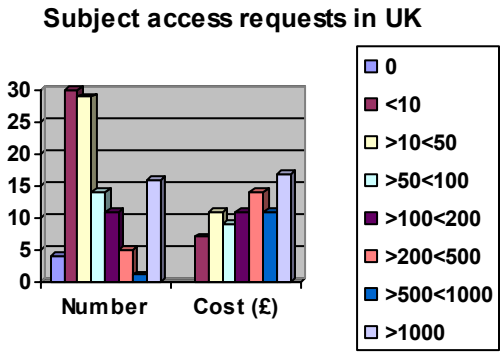
The Home Office published a subsequent regulatory assessment of the costs of implementing the Directive in 1997 [9] that estimated the start-up costs to be £1.150bn. (€1.720bn.), representing slightly more than 0.1% of GDP for the UK for that year; the annual costs were estimated to be £0.742bn. (€1.110bn), representing just less than 0.1% of the GDP. If anything, these assessments may have underestimated the impact of the inclusion of manual records in the compliance costs. The post-implementation appraisal of the Data Protection Act 1998, undertaken by the Lord Chancellors' Department in September 2000[10] did not specifically address the economics, but did include a "… *concern over the economic impact of the provision of information. As well as the cost of providing the information, the provision of information on the telephone when selling a product or service measurably resulted in abandoned calls and lost sales…"*.

Compliance with national legislation will require the data controller to manage their use of personal data. This will normally include direct costs from the need to appoint data protection officers and indirect costs associated with the provision of training and the implementation of business procedures to ensure the correct processing of data. Legislation may also limit the extent to which personal data may be shared within the organisation for different purposes from those for which it was originally collected. This will imply the need for additional resources to be devoted to increased dialogue with individual clients in order to obtain consent for the processing activities associated with these different purposes. The level of these

costs depends very much on the business sector of the organisation, but could amount to a few percent of turnover.
The elements of costs that particularly affect the public sector, apart from human resource aspects, particularly relate to the control of information sharing between government departments and the security of transactions with the citizen.
These compliance costs may be quite substantial, involving the appointment of data guardians, the development of information handling and sharing protocols and the organisation of staff training programmes. These issues are coming into prominence in tandem with the drive towards the electronic delivery of more joined-up services and can be minimised by taking the opportunity to ensure that compliance is built-in at the earliest stage to the design principles for e-government.

2.2. Individual Rights

Individuals have rights to access and to have corrected personal data processed about them by data controllers. The exercise of these rights can have costly consequences for an organisation. In order to be able to respond adequately to a subject access request, the organisation must have effective information handling processes in place.
The provision of information to data subjects is often seen as one of the more onerous requirements on data controllers. However, the extent of this burden varies substantially, depending on the type of business conducted by the organisation. Arguably, the more efficient the organisation, the lower would be the costs of the provision of information, since it should be more readily available.
In July 2002, the Department of Constitutional Affairs within the UK Government published the results of a consultation exercise on subject access that had been undertaken in the previous autumn[11].



Some of the findings of this report are illustrated in the chart opposite.
Whilst 27% of those organisations that responded had to deal with less than 10 access requests per year, 14% received over 1000 annual requests.
Only 9% of the requests were dealt with at a cost less than the subject access fee (of £10 or about €15), with over 20% costing in excess of 100 times that fee. These figures may have been skewed by the fact that over one third of the respondents were from the public sector or public bodies.
A significant element in the compliance costs arises from the inclusion of the majority of manual records within the definition of personal data. This means that organisations that hold a lot of manual records may spend a lot of effort bringing together all of this material in response to a subject access request. Recently, the Supreme Court of Appeal in the UK delivered a ruling[12] that substantially limited the types of manual data that were subject to the Law. This ruling, if carried through to general application, should have the effect of considerably reducing the burden on organisations in complying with subject access requests that might have involved searching relatively unstructured manual filing systems and accordingly reducing the high costs that have previously been quoted by some data controllers.
A similar survey conducted in 2003 throughout the European Union, "The Euro-barometer Report [13] on Data Protection in Europe" found that in 2002 49% of respondents received fewer than ten access requests per year, with less than 1% receiving in excess of 500 such requests. The vast majority (96%) of respondents received no Data Protection complaints during 2002. So, whilst the cost of dealing with an access request or a complaint may be significant when it occurs, the incidence of such requests is generally quite low, meaning that for most organisations the economic impact is also low.

2.3. Notification

The Directive requires data controllers to notify the supervisory authority of the details of their processing of personal data. Arrangements for notification vary substantially between different countries and in some cases (such as in the UK) a fee is charged; this is currently about €50 per notification.
The annual cost of the notification fee is a relatively insignificant expense, compared to the administrative time that may be required to generate the information required for a notification and the ongoing effort needed to ensure that it remains up to date. This activity would typically involve maintaining records of all systems that process personal data and being aware of all planned upgrades to such systems throughout an organisation. An integral part of the UK notification process involves the completion of a questionnaire on the security measures that are in place to protect the processing of personal data.
The costs of the overall notification process will vary and clearly could be significant for a large or complex organisation that transacts business with individuals.

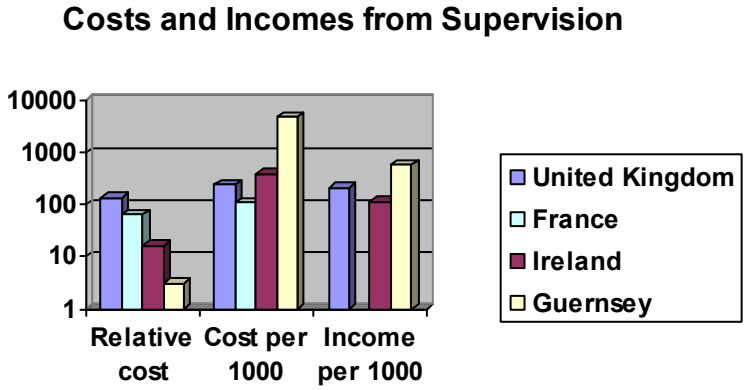
2.4. Restrictions on Data Transfer abroad

The Directive prohibits the transfer of personal data to a territory without adequate protection. Very few Third Countries have yet achieved an adequacy finding[14], so transfers in general outside the EEA can only occur under the additional protection of contractual clauses or under the authority of the national supervisory body. Contracts can take some time to negotiate and can at times be in conflict with the national law of the "Third Country", hence the need for these contracts can inhibit trade, especially between the Pacific rim and Europe, and has proved a potential barrier to activities such as outsourcing back office operations to Asian countries. The Euro-barometer report on Data Protection in Europe shows that only 10% of the companies surveyed transferred personal data outside the European Economic Area in 2002. Data Protection constraints may have been a contributory factor in this.
The European Commission's Analysis and impact study on the implementation of the Directive[15], published in 2003 found that: " *late transposition by Member States and differences in the ways the Directive is applied at national level have prevented Europe's economy from getting the full benefit of the Directive."* There was particular divergence between the national laws and practice of Member States with regard to international transfers of data and so a similar argument could be applied to postulate the harmful effects on international trade.

2.5. Supervision

In Europe, the supervisory régime is dominated by the Directive 95/46/EC.
This lays down that supervision should be by an independent statutory authority, not under direct political control. Within Europe, the Data Protection or Privacy Commissioner's office is normally funded by central or regional government and in some cases may charge fees for its services such as for maintaining a register of data controllers. Such fees payable by law to a public body are essentially a form of indirect taxation and so any fee income should ideally be disregarded when international comparisons of the costs of the supervisory régimes are made.
The federal or regional structure of some European states further complicates a comparative study of costs as does the different functions performed by such supervisory bodies – in the UK, for example, the Information Commissioner is responsible for enforcing Freedom of Information legislation as well as Data Protection. The chart below illustrates the comparative costs of regulation in the UK, France, Ireland and Guernsey.
In the UK, which is the largest non-federal Member State in the EU, the Information Commissioner's Office spent about €14m in 2003,[16] which is €240.00 per thousand head of the population. That cost was largely offset by income of about €12.5m. (€212 per thousand).
Similarly, the 2003 budget of the CNIL in France was €6.5m[17], representing €108 per thousand head of the population for a mandate that was more specifically concerned with privacy.
By way of contrast, in the Republic of Ireland, which is one of the smaller Member States, the Data Protection Commissioner's Office[18] spent about €1.6m in 2003 (€404.00 per thousand) as against an income of €0.45m. (€115 per thousand).

In Guernsey[19], which has a population of only 60,000, last year I spent about €288,000 (€4,800 per thousand) against a income from fees of €35,000 (€583 per thousand).
These figures serve to illustrate the economies of scale that can apply to larger countries.



3. Benefits

So, let us look at the benefits of regulation, under similar headings that we used for examining the costs.

3.1. Compliance with the Principles

Compliance with the principles can have a significant impact on business processes and business organisation. Organisations that show that they are compliant with the principles should derive a number of benefits, including:

- Better staff relations, through improved transparency of personnel records and improved training;
- Better customer relations, through improved record keeping and up-to-date information and enhanced consumer confidence;
- Fewer complaints from clients, resulting in lower overhead costs;
- More efficient operations through better organised filing systems and improved business processes;
- Improved opportunities to transact international business, especially with customers resident in EU Member States.

3.2. Individual rights

Incorporation of respect for human rights, especially the right to privacy, into national law contributes to the establishment of a fair, just and open society.
This legislation means that citizens who transact business with government will have increased confidence that their personal information will be respected and will not be unnecessarily shared without their consent.
It has been widely predicted that e-commerce will continue to grow to encompass more and more consumer-led transactions. E-commerce itself offers amazingly low transaction costs, especially where services, such as theatre bookings, tickets for public transport and music downloads are concerned. The economic consequences of the widespread adoption of e-commerce are immense. However, its growth has not nearly been as rapid as was predicted and one reason for this is the lack of trust by consumers in doing business over the Internet.
Consequently, it can be argued that exploitation of the strong regulation of Data Protection can have a pivotal role to play in facilitating the increased confidence amongst consumers that their personal data will not be abused from the use of electronic transactions.
Organisations established throughout Europe are able to exploit their compliance with strong Data Protection legislation to offer improved levels of consumer protection and should therefore be able to gain substantial competitive advantage from e-commerce applications. The high profile given to personal privacy within Europe can mean that European consumers may be discouraged from doing business over the Internet unless they can be sure that the privacy of their business is protected by adequate legislation in the destination country.

3.3. Notification

There are no particularly obvious direct economic benefits from the notification process. Indeed there are many who think that notification is a waste of time. Although it does consume some resources, the side effects of notification can be a greater awareness amongst the business community of Data Protection matters and the incentive to establish an organisational focus for everything concerned with personal data. As an example, completion of the security questionnaire that is associated with the notification processes forces an organisation to consider its security procedures and is in itself an educational exercise. Notification can also reduce the need to respond to the more straightforward requests for information about processing, as the answers to such requests may be found in the published notification; hence individuals can know at the outset the types of information processed and purposes for which they are processed prior to deciding whether it is necessary to make a detailed subject access request.

3.4. Restrictions on Data Transfer abroad

As has been previously mentioned, the prohibition of data transfers to non-adequate jurisdictions can initially have negative economic consequences as it can restrict trade, by making it more difficult to do business with organisations based in such territories.
This is very much a short-term view. In whatever field standards are introduced they have the effect of partitioning the universe into the compliant and the non-compliant. Once it has been recognised that the standards are worthwhile, they become more universally adopted, with the result that economic costs of non-compliance far outweigh the costs of compliance.
Essentially, this means that the pressure on a country to enact legislation to provide adequate Data Protection is increased as a result of the economic effect of the trade sanctions that it suffers. Certainly, it was economic arguments that were primarily used to justify updating the Data Protection legislation in Guernsey, such that we were able to obtain a finding of adequacy.
However, with much of the United States, Latin America, Africa and Asia not yet deemed "adequate" by the European Commission, we are still some way from reaching a critical mass of "adequate" economies that would enable sufficient pressure to be imposed to facilitate the free movement of personal data on a global scale. Indeed, there is a danger that the reverse could apply – strong economic pressure by those with "weak" protection might be applied in an effort to dilute the level of protection that applies in Europe and those other countries that enjoy "strong" protection.

3.5. Supervision

The supervisory body imposes a direct and an indirect load on the taxpayer. What benefits accrue from having an independent supervisor? For the regulation of business, it of little concern whether the regulator is a government servant or not. For the regulation of government, of course, it is vitally important that regulation can be seen to be independent and promoting the right balance between the legitimate needs of the state and the fundamental rights of the individual. Striking this balance is particularly relevant at the present time in dealing with the responses to international terrorism and money laundering and in the debate over biometrics, identity cards and the interception of communications.
One of the major functions of the supervisory body is that of increasing public awareness – this translates into enhanced public confidence and improved quality of life. Intangible benefits, but benefits none the less. More tangible is the power of the regulator to intervene, to respond to complaints, to enforce compliance - normally without the need to exercise the legal process by engaging in prosecution or litigation. This may be bad news for the legal profession, but it is good news for the economy, as most problems can be fixed by intervention rather than confrontation. By way of example, in 2003 the UK Information Commissioner processed approximately 12,000 complaints, involving nearly 5,000 assessments of processing, but undertook only eight prosecutions.

4. Conclusions

The protection of privacy has long been recognised as having important economic consequences and has been high on the agenda of intergovernmental organisations such as the OECD and the Council of Europe for over 25 years. The processing of personal data in Europe is subject to strong regulation driven by the EU Directive that interferes in the free market by imposing high standards on the processing and protection of Personal Data in both the private and public sectors.
Strong regulation appears to have a significant economic cost, which although amounting to a fraction of a percent of a nation's Gross Domestic Product, may have a greater indirect effect by inhibiting the capacity of that nation to trade internationally. However, this cost is balanced by the increased consumer trust in dealing with an economy that respects privacy.
Although the European Commission has undertaken an analysis of the implementation of the Directive, this did not extend to an economic appraisal. However, it is understood that the Commission is in the process of commissioning a study into the costs of compliance, the results of which should be available in 2005.
Whilst some countries have followed the European approach, many other countries have favoured a regulatory approach that depends more on voluntary compliance, with sectoral legislation addressing areas of particular concern. This difference in approach could inhibit the flow of personal data between the "strong" and "weak" regulatory environments and is particularly relevant to consideration of the needs of international ecommerce.
In its 2004 economic survey of the Euro area[20], the OECD reports: *"Goods, services and financial market integration must be deepened with a view to raising that area's growth potential"*. Implicit in that statement is the need for common global privacy standards to facilitate trans-border flows of personal data.
The final report of the World Summit on the Information Society[21] the important role of privacy protection is recognised in Principle 35. "*Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society*."

There is currently very little data available on the costs of complying with privacy regulation and even less on its economic benefits. The benefits of strong regulation are mostly intangible, but contribute towards the creation of a fair and open society. The question remains – are the costs balanced by the benefits?

Bibliography

[1]The text of the declaration may be found at:
http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
[2] A description of this publication may be found at:
http://www.oecd.org/document/49/0,2340,en_2649_33703_19216241_1_1_1_1,00.html
[3] Further information on the privacy policy of the OECD and the privacy statement generator may be found at www.oecd.org/privacy .
[4] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data http://conventions.coe.int/Treaty/en/Treaties/Word/108.doc
[5] Directive 95/46/EC on the protection of individuals with the regard to the processing of personal data and on the free movement of such data OJ L 281 23.11.95 p 31-50. http://europa.eu.int/comm/internal_market/privacy/law_en.htm
[6] Costs of Implementing the Data Protection Directive. Paper by the United Kingdom. Home Office 1994.
[7] Data Protection News, Issue 20 Winter 1994/95, published by Hoskyns (CAP Gemini Sogeti)
[8] Report to the European Commission: An Evaluation of the Financial Impact of the Proposed European Data Protection Directive, Ashton Business School, 1994

[9] Regulatory Impact Assessment of Directive 95/46/EC, Home Office December 1997
www.dca.gov.uk/ccpd/dpara.htm
[10] Data Protection Act 1998 Post-Implementation Appraisal CP(R)99/01 originally published by the Lord Chancellor's Department, December 2001 http://www.dca.gov.uk/ccpd/dparesp.htm
[11] Response to the Consultation Paper - Data Protection Act 1998:Subject Access, July 2003
www.dca.gov.uk/consult/foi/dpsaresp.htm
[12] Michael John Durant v Financial Services Authority [2003] EWCA Civ. 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003.
http://www.courtservice.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm
[13] EOS Gallup Europe Flash Eurobarometer 147 "Data Protection in the European Union":
http://europa.eu.int/comm/public_opinion/flash/fl147_exec_summ.pdf.
[14] Commission decisions on adequacy may be found at:
http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm
[15] European Commission's First Report on the transposition of the Data Protection Directive, 26 May 2003
http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm
[16] Annual Report and Accounts of the UK Information Commissioner for 2003
http://www.informationcommissioner.gov.uk/cms/DocumentUploads/AR03.pdf
[17] CNIL 24e rapport d'activité 2003, Annexe 4
[18] Fifteenth Annual Report of the Data Protection Commissioner for the Republic of Ireland for 2003
http://www.dataprivacy.ie/images/annual_report_2003.pdf
[19] Bailiwick of Guernsey Data Protection Commissioner's report for 2003
http://www.dataprotection.gov.gg/Reports/2003%20Report.pdf
[20] www.oecd.org/dataoecd/17/33/33626607.pdf
[21] Final Report of the Geneva Phase of the Summit WSIS-03/GENEVA/DOC/0009 (rev. 1)
http://www.itu.int/wsis/documents/doc_multi-en-1191|0.asp