Is a global data protection regulatory model possible ?

de Terwangne , Cécile

Published in:
Reinventing data protection ?

Publication date:
2009

Document Version
Publisher's PDF, also known as Version of record

Chapter 10
Is a Global Data Protection Regulatory Model Possible?

Cécile de Terwangne

10.1 Introduction

On 14 September 2007 Peter Fleischer, Google's global privacy counsel, pleaded at a UNESCO conference for the setting up of global international privacy standards. At the same time, in parallel, he posted the following text on Google Public Policy Blog:

'Google is calling for a discussion about international privacy standards which work to protect everyone's privacy on the Internet. These standards must be clear and strong, mindful of commercial realities, and in line with oftentimes divergent political needs. Moreover, global privacy standards need to reflect technological realities, taking into account how quickly these realities can change.'

Such an advocacy of privacy was clearly an essay from Google's officials to regain prestige notably after the revelation that Google had been keeping and using huge amounts of personal data collected from users' web researches.[1] Anyway, whatever the strategy and the sincerity of the appeal, it has had a worldwide repercussion due to the fact that it emerged from the largest web search engine company.

Precisely two years before, on 14 September 2005, a similar call for global harmonization of the protection of information privacy was launched by the world's

C. de Terwangne (✉)
Faculty of Law, University of Namur, Namur, Belgium
e-mail: cecile.deterwangne@fundp.ac.be

[1] At the same time Google was trying to buy DoubleClick, the largest cyber-marketing company. This prospect of merging two huge data bases mobilized (real) privacy advocates who put forward the severe risk for privacy that such an operation would represent: 'On April 20 2007 the Electronic Privacy information Center (EPIC) filed a complaint with the US Federal Trade Commission to block Google's planned acquisition of Internet advertiser DoubleClick. [...] Google is the internet's largest search company. DoubleClick is the internet's largest advertising company. Neither has done a particularly good job protecting online privacy and the combined company would pose a unique and substantial threat to the privacy interests of internet users around the globe.' M. Rotenberg, 'Google's proposals on internet privacy do not go far enough', *Financial Times*, 24 September 2007.

S. Gutwirth et al. (eds.), *Reinventing Data Protection?*

DOI 10.1007/978-1-4020-9498-9_10,

privacy and data protection Commissioners at their annual international conference in Montreux, Switzerland. They adopted the Montreux Declaration entitled 'The protection of personal data and privacy in a globalized world: a universal right respecting diversities'.

In this text, the privacy Commissioners stated that 'It is necessary to strengthen the universal character of this right in order to obtain a universal recognition of the principles governing the processing of personal data whilst respecting legal, political, economical and cultural diversities'. In addition, the Commissioners have agreed to work towards this recognition of the universal nature of data protection principles. They committed themselves to work with governments as well as international and supranational organisations with a view to adopting a universal convention on data protection.

This declaration did not reach a wide public for sure but there is no doubt about the sincerity and conviction of its authors.

In fact one could advocate that such international privacy standards have already been defined since more than a quarter of century.[2] On 22 September 1980, the Organisation for Economic Co-operation and Development (OECD) published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[3] And on 28 January 1981 the Council of Europe adopted the Convention for the protection of individuals with regard to automatic processing of personal data.[4] These international texts contain what can be considered as the fundamental information privacy principles.

So the question can be put whether there is still a need of global harmonization of privacy/data protection standards. And if such a need exists, what could be the content of such a global data protection model?

10.2 Is There a Need of Global Harmonization of Data Protection Regimes Throughout the World?

The answer to the question about the real necessity of a harmonised and universal protection of personal data is linked to the characteristics of the world in which we live today, the so-called 'information society'. We are facing an ever-increasing need of free flows of data (1.1.) whereas new risks and threats arise from the development of information technologies (1.2.).

[2] See for example Marc Rotenberg's sarcastic reaction to Google's proposal for international standards of privacy protection online: 'This is an interesting proposal, since countries from America, Europe and Asia announced global privacy standards more than 25 years ago.' (op. cit.).

[3] Available at: <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[4] Available at: http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/international_legal_instruments

10.2.1 Increased Need of Free Flows of Data

Globalization of business and extensive developments of global information networks have intensified a need that was already identified in 1980. In fact, at that time when the OECD Guidelines were adopted, it was already with a view of guaranteeing the free flows of personal information so that business activities could be run properly. A need of sharing personal data, communicating them across boundaries was already induced by the international movements of goods and services, multi-place economic activities and the deploying of multinationals.

This trend of internationalizing business, marketplaces and organisations has been accelerating these last decades and has lead to the phenomenon of 'globalization'. In a concomitant way, the need to have personal data free to be transferred through national frontiers grew as well. Data are effectively linked to the flows of goods, services, finance, to the movement of persons and workers, etc.

We live nowadays in a globalized but also in a networked society. Technical interconnection has brought with it human interconnection (for professional, social, economic, political, personal, etc., reasons). The deployment of the Internet has drastically increased the possibilities of exchange of information. The technical means of international exchanges are now available to ordinary individuals. We see official as well as private websites, blogs, forums, social network sites and virtual communities flourish. Moreover, information and communication technologies – the Internet in the first place – generate additional and most of the time hidden flows of data, some of which are necessary for the offer of the information service or help to the management of the service while others are exploited for their potential economic value.

Finally, since the events of the 11th of September 2001 the globalized and networked society has become a cross-border surveillance society. Henceforth flows of personal data concern national and trans-national police and surveillance services more and more interested in the sharing and the communication of personal information.

10.2.2 Higher Risks and Threats

International flows of personal data are a clear reality as well as the need for such flows not to be disrupted. But this reality goes together with higher or even new risks and threats with regard to the individuals' freedoms and rights.

The globalization of economic activities has caused the intensification of cross-borders information exchanges. This means a practical difficulty for the data subjects to follow the personal information concerning them, to control who does what with it and to verify the quality of data and its relevance as regards the aim of the processing. Geographical distance goes with loss of track of data, difficulty to find the right interlocutor, language difficulties and difficulty to be listened to and respected. In addition to this reduction – in fact deprivation – of mastery over one's

personal data, means of redress are not always available or affordable in countries where data are transferred.

Information networks and especially the Internet, have in a certain measure suppressed any geographical dimension, which increases the difficulty to be aware of things and to keep control over one's personal data once they have been communicated through the network.

Besides that risk of control deprivation, one watches the multiplication of uses of intrusive technologies of data processing and of hidden collections and uses of personal data. The Internet surfer leaves a trail of personal details, which are captured by computer logs. This involuntary mine of information notably allows personalized cyber-marketing. Surveillance at work through telecommunications control or through cameras has rapidly followed technical progress. The introduction of Internet connections and of e-mail possibilities in the offices has been accompanied by surveillance of web surf and of e-mail use.[5] Localization data, behaviour data and biometric data are also being processed for different purposes among which is surveillance. The spread of RFID (Radio Frequency Identification[6]) offers an additional way of invading individuals' privacy.

The increase of security concern has also brought with it an intensive recourse to invasive control technologies. Video surveillance has expanded everywhere and is more and more refined (with zoom possibilities, night vision, face recognition technology, detection of unusual behaviour or suspect profile etc.). Travel is a major opportunity for control either through the processing of localization data or through the collection and long-term storing of huge quantity of details about each traveller (air passengers, see the PNR problem).[7]

10.3 Disparities Between Legal Data Protection Regimes

In response to the technological progress and developments, to the reality of ever-increasing uses and movements of personal data and to the ensuing risks for civil liberties and rights, especially for privacy, answers can be found in data protection legislation. However, existing models of data protection are pretty diverse.

[5] For a detailed overview of technological control on workplace see Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006, an International Survey of Privacy Laws and Developments*, Washington, DC, EPIC, 2007, pp. 65–79.

[6] See 'What is Radio Frequency Identification (RFID)?', AIM Global, Association for Automatic Identification and Mobility, http://www.aimgobal.org/technologies/rfid/what_is_rfid.asp

[7] See Article 29 European Data Protection Working Party, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), January 29, 2004, available at http://ec.europa.eu/justice_home/fsj/privacy/ workinggroup/wpdocs/2004_en.htm; Privacy International et alii, *Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection*, February 2004, available at http://www.privacyinternational.org/issus/terrorism/rpt/transferringprivacy.pdf

10.3.1 The Comprehensive Model

The European Union has adopted a comprehensive regulatory model. The common legal framework for the 27 EU Member States lays mainly in the general Directive 95/46/CE[8] elaborating the general data protection regime, completed by specific Directives 2002/58/CE[9] on privacy and electronic communications and 2006/24/EC[10] , the so-called Data Retention Directive. These texts aim at warranting the free flow of personal data inside the European Union together with offering guarantees as to the protection of those data in name of the protection of an authentic human right.[11]

On the basis of these texts harmonized and comprehensive data protection legislation has been enacted in all the 27 EU Member States. This legislation sets rules concerning the legitimacy of data processing, data quality, the protection of sensitive data, transborder data flows, the accountability and enforcement ways and notably, the role of independent data protection authorities. It grants specific rights to the data subjects and imposes duties to data controllers as regards data processing.

10.3.2 The Piecemeal Model

The United States have followed a totally different approach far from the European model of an all-encompassing protection regime. The U.S. system is complex, associating federal and state level regulations and self-regulatory and co-regulatory measures. Adopted legislations are sector-oriented (for example ruling the health[12] or the financial sector[13]) or address specific and sometimes narrowly-targeted privacy issues (for instance the video privacy Protection Act).[14] This fragmented system of protection presents the disadvantage of inevitable gaps in protection and

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281, 23.11.1995, p. 31–50.

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ*, L 201, 31.7.2002, p. 37–47.

[10] 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, *OJ*, L 105, 13.4.2006, p. 54–63.

[11] See Article 8 of the Charter of Fundamental Rights of the European Union recognizing the 'right to the protection of personal data' aside from the 'right to respect for [one's] private and family life, home and communications' (Article 7 of the Charter).

[12] Health Insurance Portability and Accountability Act ('HIPPA'), 45 C.F.R. §§ 160–164.

[13] Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422; Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq.; Gramm-Leach Bliley Act, 15 U.S.C. §§ 6801–6809.

[14] Video Privacy Protection Act, 18 U.S.C. 2710. see J. R. Reidenberg, 'Privacy Wrongs in search of Remedies', 47 *Hastings L.J.* 877 (2003).

in enforcement or leads to anomalies.[15] Enforcement mechanisms particularly raise criticisms since some regulations exclude the possibility of direct complaint by individuals. Launching complaint is reserved to organizations acting on behalf of the consumer: the Federal Trade Commission (FTC) or the Federal Communications Commission (FCC), for instance.

Labelling schemes offer an example of self-regulation (such as TRUSTe or BBBOnline). They have been developed to certify and monitor privacy policies adopted by a labelled organisation.

The Safe Harbor Principles agreement signed between USA and EU[16] illustrates the co-regulation phenomenon. Organisations are only submitted to the principles contained in the agreement if they decide so. Official bodies like FTC are entitled to sue infringements to the principles.

10.3.3 The sector-Oriented Model

Some other countries like Japan, Australia or New Zealand, have focused on sector specific and local rules: they have adopted relatively comprehensive laws establishing general fair information principles (on the OECD model) and have subsequently elaborated these principles in numerous sectors regulations. They equally foster self-regulation.

10.3.4 The 'Risk-Burden Balance' Model

Japan's and Australia's model is also characterised by the fact that their legislation exempts ranges of activities because they consider them as presenting no danger that would deserve an answer in terms of protection of individuals. The Australian Privacy Act 1988 exempts all the small businesses from respecting the National Privacy Principles.[17] In Japan, entities that have been holding personal information on less than 5,000 individuals or for less than 6 months are exempt from regulation.[18]

10.4 Disparities in the Ways of Considering Data Protection

There are various ways to consider data protection. These divergent considerations have an impact on the attitude adopted towards the problem of data protection.

Data protection can be seen as a fundamental right. That is clearly the Council of Europe's approach and the European Union's approach in general: the Council of

[15] For example, cable service providers are regulated differently from Internet service providers.

[16] Decision 2000/520/CE, *J.O.C.E.*, 25 August 2000, L 215, pp. 0007–0047.

[17] See Section 6D of the Privacy Act 1988 that defines what is to be considered as 'small business'.

[18] Act No. 57 on the Protection of Personal Information, May 30, 2003.

Europe Convention 108 and Article 8 of the EU Charter of fundamental rights are evident human rights instruments. The EC directives on data protection are the result of the necessity to manage a human right in the framework and with the constraints of a global market.[19]

Far from this perspective, data protection can be considered as a consumer concern. Following this point of view, personal data are marketable goods and the protection of this data is to be balanced with private interests. This leads to no real rights being guaranteed to the data subject: individual access to one's personal information may be refused when there is an overriding private interest or when the burden it would lead to would be disproportionate to the risks. This is the perception underlying the model of APEC Privacy Framework[20,21] as well as the EU-US Safe Harbour agreement.[22]

Data protection can also be perceived as just a problem of trust. Data protection is then reduced to a question of security. The World Summit on the Information Society Declaration in 2003[23] follows this point of view and treats data protection as part of cyber-security. Data protection coincides with confidentiality and confidentiality breaches are the problem to tackle.

[19] See Article 1 of the Directive 95/46: '1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

[20] Asia Pacific Economic Countries (APEC) Privacy Framework, November 2004 – Available at <http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html>

[21] The VIIIth APEC's privacy principle entitled 'Access and Correction' avoids the word 'right'. It states 'Individuals *should be able to*: (a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; (b) have communicated to them, after having provided sufficient proof of their identity, personal information about them [...]; (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

Such *access and opportunity for correction* should be provided *except where:* (i) *the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question*; (ii) the information should not be disclosed due to [...] or *to protect confidential commercial information*; or (iii) [...].'

[22] Decision 2000/520/CE, *J.O.C.E.*, 25 August 2000, L 215, pp. 0007–0047.

[23] World Summit of the Information Society, Declaration of Principles – Building the Information Society: a global challenge in the new Millennium, Document WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003: 'B 5 Building confidence and security in the use of ICTs 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.'

10.5 A Universal Data Protection Model?

10.5.1 Existing International/Regional Standards

10.5.1.1 OECD's Guidelines

As mentioned in the Introduction of this paper, OECD is the first international arena where a consensus between several states, major economic actors and as such intensive users of (personal) information, could be reached. This has lead to the publication of the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[24] These Guidelines contain what is known as the fundamental fair information principles, eight principles that have inspired many legislation or self-regulation documents around the world. These principles are the following ones: (1) collection limitation, (2) data quality, (3) purpose specification, (4) use limitation, (5) security safeguards, (6) openness, (7) individual participation and (8) accountability.

The 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' adopted by the OECD Council on 12 June 2007 also stresses the need to reach a common protection of personal data throughout the world. It states 'This Recommendation is intended to foster international co-operation among Privacy Enforcement Authorities to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located. It reflects a commitment by member countries to improve their enforcement systems and laws where needed to increase their effectiveness in protecting privacy.'[25]

10.5.1.2 Council of Europe's Convention

The second multi-national instrument dealing with data protection, already mentioned in the Introduction as well, was adopted only four months later. It is the Council of Europe Convention 108 (28 January 1981) for the protection of individuals with regard to automatic processing of personal data. This text promotes basic principles for data protection. Unsurprisingly these principles are in the line of those proclaimed by OECD. Some divergences are noticeable. The Council of Europe instrument establishes special categories of data, provides additional safeguards for individuals and requires countries to establish sanctions and remedies. The Convention has been completed ten years later by an additional Protocol[26] to insist on the role of independent supervisory authorities and to take into consideration the increase in exchanges of personal data across national borders.

[24] See Sjaak Nouwt's contribution in the present book.

[25] Point 2 of the Annex. Available at <www.oecd.org/sti/privacycooperation>

[26] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001.

10.5.1.3 United Nations' Guidelines

UN Guidelines for the Regulation of Computerized Personal Data Files (Resolution 45/95 1990) have been adopted on 14 December 1990. These guidelines contain minimum guarantees in data protection field that should be provided in national legislation. These guarantees are expressed in a set of general principles pretty similar to the fair information principles already recognized in the previous international/regional instruments. These principles are:

1. Principle of lawfulness and fairness;
2. Principle of accuracy;
3. Principle of the purpose-specification;
4. Principle of interested-person access;
5. Principle of non-discrimination: special categories of information should not be collected;
6. Admissible exceptions;
7. Principle of security;
8. Supervision and sanctions;
9. Transborder data flows: they should be free to countries with comparable guarantees.

10.5.1.4 Asia Pacific Economic Cooperation (APEC)'s Privacy Framework

Peter Fleisher, Google's global privacy counsel, added in his pleading for the adoption of information privacy protection universal standards 'To my mind, the APEC privacy Framework is the most promising foundation on which to build. The APEC framework already carefully balances information privacy with business needs and commercial interests. And unlike the OECD guidelines and the European Directive, it was developed in the Internet age.' Are APEC principles really good global data protection standards?

Graham Greenleaf does not share Peter Fleisher's enthusiasm about the APEC Framework 'The privacy principles are at best an approximation of what was regarded as acceptable information privacy principles 20 years ago when the OECD Guidelines were developed', he stated.[27] Neither does Marc Rotenberg, convinced that 'APEC Framework is backward looking. It is the weakest international framework for privacy protection, far below what the Europeans require or what is allowed for trans-Atlantic transfers between Europe and the U.S.', particularly because it focuses on the need to show harm to the consumer.[28]

In fact APEC's Privacy Framework, even if based on the OECD Guidelines consensus, does not reproduce all the content of these Guidelines: it has dropped the

[27] G. Greenleaf, 'Asia-Pacific developments in information privacy law and its interpretation', *University of New South Wales Faculty of Law Research Series* 5 (19 January 2007).

[28] Marc Rotenberg, op. cit.

Openness Principle[29] and has lowered the content of other principles such as the Purpose Specification Principle[30], for example. It has also not reproduced principles present in other international instruments or in national laws of many countries among which are APEC's Member States.[31,32]

Moreover, new principles have appeared, testimony of the influence the USA have had on APEC's negotiation process. The principle of 'Choice' for instance that could already be found in the EU-US Safe Harbour Agreement. It provides that 'Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information'. This principle can present a danger of lessening the protection if implemented in certain ways, notably if it mainly means 'opt-out principle.'[33] The 'Preventing harm' principle is also a new 'protection' principle susceptible of dangerous application. It says that 'Personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information'. Such a principle can be used to justify exempting whole sectors of activities (as the small businesses sector in Australian law) because of not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the USA).[34] It can also lead to

[29] 'Openness Principle (12). There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.'

[30] 'Purpose Specification Principle (9). The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.' In contrast, the APEC Information Privacy Principle entitled 'Notice' provides that clear statements should be made accessible by information controllers, disclosing the purposes of collection, possible types of disclosures, controller details and means by which an individual may limit use and disclosure and access and correct their information. 'All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable'.

[31] For instance, it does not limit collection to lawful purposes.

[32] On all the critiques about the weaknesses of APEC Privacy Framework, see G. Greenleaf, 'APEC's Privacy Framework sets a new low standard for the Asia-Pacific', in M Richardson and A Kenyon (Eds) *New Dimensions in Privacy Law: International and Comparative Perspectives*, Cambridge University Press, 2006, pp. 91–120; G. Greenleaf, 'Asia-Pacific developments in information privacy law and its interpretation', op. cit.

[33] In the FAQ linked to the Safe Harbor Principles, it is clearly stated that choice means opt-out, except for sensitive data.

[34] G. Greenleaf, 'APEC's Privacy Framework sets a new low standard for the Asia-Pacific', op. cit., p. 100.

the necessity for individuals to prove the risk of harm to obtain the benefice of protection.[35]

Finally, APEC Framework excludes information that may be used to enter into contact with somebody from the scope of the definition of 'personal information'. This is 'an illustration of where APEC's principles look to the past and do not deal with problems of the present and future.'[36] Indeed, among the information not covered by the protection fall phone numbers, email addresses and IP addresses.

Even if the last born of the international instruments that govern data protection, the APEC's Privacy Framework should not serve as a model for a universal set of data protection standards.

Having observed the international panorama of data protection instruments, we can conclude that there are commonly accepted core principles, certain of which could be called 'content principles' while others address the problem of enforcement of the content principles. But these principles have appeared in the two last decades of the XXth century, before the expansion of world-wide networks like the Internet. A positive and a negative point can be made about this. These long-lasting data protection principles have proved to be capable of adapting to the evolution of technology and reality. They are still an adequate answer to the problems and risks arisen from the technological developments. However, they do not answer to all the new threats induced by these developments. In the last paragraphs of this contribution we will list the admitted core principles, content ones and enforcement ones and evoke the emerging additional principles that should be soon part of the universal data protection standards.

10.5.2 Universal Standards: Content Principles

10.5.2.1 Collection Limitation Principle

There should be limits to the collection of personal data. Only personal data that are relevant to the purposes for which they are to be used should be collected.

Moreover, personal data should be collected lawfully and in a fair manner, which means that data should be collected transparently, not about data subjects who would not be aware of the operation.

10.5.2.2 Data Quality Principle

In addition to be relevant as regards the collection purposes, data should be accurate, complete and kept up-to-date to the extent necessary for those purposes.

[35] 'He would also place on Internet users the burden of showing how and where harm occurred, which is particularly unfair since so little is known about how companies that collect personal data make use of the information.' M. Rotenberg, op. cit.

[36] G. Greenleaf, APEC's Privacy Framework sets a new low standard for the Asia-Pacific', op. cit., p. 100.

10.5.2.3 Purpose Specification and Limitation/Use Limitation Principle

The purposes for which personal data are collected should be specified. It should not be allowed to store data for undefined purposes. The subsequent use must be limited to the fulfilment of those purposes or such others as are not incompatible with the initial purposes.

10.5.2.4 Non Discrimination (Sensitive Data)

Certain categories of personal data more likely than others to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled except in certain limited cases.

10.5.2.5 Security Principle

Data should be offered adequate security safeguards with regard to the risk involved and the nature of the data. Organisational measures (for instance the restriction of access to the information within the organisation, or requirements concerning long-term storage) as well as technical measures have to be taken. They should be based on the current state of the art of data security methods and techniques in the field of data processing.

10.5.2.6 Openness Principle

Personal data controllers should provide clear and easily accessible statements about their practices. Individuals should be provided with information as to the identity of the data controller, the purpose of the processing and the categories of disclosures of the data.

10.5.2.7 Individual Participation Principle (Right of Access and of Correction)

Everyone who proofs his/her identity must be recognized the right to know whether information concerning him/her is being processed and to obtain it in an intelligible form, without undue delay or expense. He/she must have the right to have erroneous or inappropriate or unlawful data rectified or erased.

10.5.2.8 Responsibility/Accountability Principle

Personal data controllers should be responsible for unlawful data processing.

10.5.2.9 Proper Level of Protection in Case of Transborder Flows

Transborder data flows to countries that offer comparable safeguards for the protection of personal data should not be hampered.

10.5.3 Universal Standards: Enforcement Principles

'If you haven't got compliance, you haven't got much.'[37]

10.5.3.1 Independent Supervision

Each country is invited to designate an authority responsible for supervising observance of the principles set forth above. These authorities shall offer guarantees of impartiality and independence vis-a-vis persons or agencies responsible for processing data.

10.5.3.2 Legal Sanctions and Remedies

In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

10.5.4 Additional Principles

10.5.4.1 Minimisation Principle

The collection limitation principle should be rewritten to integrate also a dimension already present in various national legislations: the minimisation of collection of data. The obligation to reduce to a minimum the data collected to feed a data processing has become especially important, notably to guide technical developers of information products.

10.5.4.2 Proportionality Principle

Unlike the APEC's approach that could be seen as using the proportionality principle to restrict the scope of data protection regulation, we propose to integrate this principle inside the scope of the protection.

The purpose should be specified (purpose specification principle) but it should also be asked that the purpose be legitimate. This requirement is present in the Council of Europe Convention 108, in the EU data protection general Directive (and consequently in the national legislation of the 27 European Member States) and in the UN Guidelines. This is the expression of the proportionality principle. It means that to be considered as legitimate a data processing should not cause more harm to the data subject than it presents interest to the data controller.

---

[37] Peter Hustinx at the International Conference 'Reinventing Data Protection?', Brussels, 12 and 13 October 2007.

The proportionality principle has also implications on the collected data. Only non excessive data should be collected. Data although relevant as regards the purpose of the processing, should not be collected if its collection or use would cause too much harm to the data subject.

10.5.4.3 Right to Know the Logic

At the Brussels Conference, Marc Rotenberg said in a fairy tale way: 'There is a giant sleeping in the EU directive. That is the right to know the logic of a data processing'. He meant Article 12 of the 95/46 EU Directive that states: 'Right of access:

Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- *knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1)*; (. . .).'[38]

It is true that what was introduced in the EU directive was an answer to the development of automated decisions. But such a right should not be restricted to automated decision. It should be effective towards any personal data processing. Individuals should be given the right to know the logic involved in any processing of data concerning them. This is extremely important in presence of profiling activities.

10.6 Conclusion

There already exist commonly accepted data protection standards. They have been tested for more than twenty years and have proved to be adaptable to technological change. The last international instrument about data protection, the APEC Privacy Framework, is however a weakening of these standards, certainly due to the influence of the USA in the negotiation process. The US have a market-oriented approach to the question and hardly accept imposing 'burdens' on economic activities in the name of the protection of personal data. This last instrument, even with its imperfections, is nevertheless a sign of the expansion throughout the world of

[38] Our italics.

the concern about data protection. The development of the Internet has rendered this concern critical. ICT developments in general and the tremendous growth of their use in all human activities (social, economic, political, etc.) have also shown the necessity to enrich the fundamental data protection principles with additional principles meant to maintain the balance between the efficiency of the technological tools and the power of their users on the one hand and the rights and interests of the individuals, data subjects, on the other.