Privacy and Data Protection in an International Perspective

Lee A. Bygrave

1 Introduction

This article provides a cross-jurisdictional review of the development of regulatory instruments (statutes, recommendations, guidelines, etc.) to protect privacy and related interests with regard to the processing of personal data.[1] In Europe, such instruments tend to be described in terms of "data protection" – the nomenclature that is mainly used in this article too. Outside Europe, the preferred nomenclature tends to be protection of "privacy", "data privacy" or "information privacy". Regardless of these terminological differences, all of the instruments constituting the focus of this article are specifically aimed at regulating the processing of data relating to, and facilitating identification of, persons (i.e., personal data) in order to safeguard, at least partly, the privacy and related interests of those persons. The central rules that are herewith applied to the processing of such data embody a set of largely procedural, "fair information" principles stipulating, *inter alia*, the manner and purposes of data processing, measures to ensure adequate quality of the data, and measures to ensure that the processing is transparent to, and capable of being influenced by, the person to whom the data relate ("data subject").

Taken together, these instruments form a field of law and policy that has attained considerable maturity, spread and normative importance over the last four decades. Well over forty countries have now enacted relatively comprehensive data protection laws. These national initiatives are augmented and often inspired by a large number of international agreements. Enveloping the regulatory field is an immense body of academic commentary analysing privacy and data protection issues from a variety of perspectives.

Thus, the global data protection scene is exceedingly complex and it is well beyond the scope of this article to depict accurately all of its nooks and crannies. The article's principal remit is: (i) to present and compare briefly various national, regional and cultural conceptualisations of the ideals and rationale of privacy and data protection; (ii) to outline the central international and national laws in the data protection field, highlighting at the same time their main similarities and differences. For the most part, the analysis is broad-brush. Thus, the article tends to steer clear of examining in detail the rules and principles contained in the instruments concerned. Effort is directed rather at summing up basic regulatory patterns in the global data protection scene, the focus being the "big picture".

1 The article is an updated and extended version of the author's earlier work on point: *see* Bygrave, L.A., *Privacy Protection in a Global Context – A Comparative Overview*, Scandinavian Studies in Law 2004, vol. 47, p. 319–348. The latter article builds on a report by the author that was commissioned in 2003 by the U.S. National Academies as part of their study on "Privacy in the Information Age". An edited version of that report was published (with the title "International Perspectives on Privacy") as Appendix B to Waldo, J., Lin, H.S. and Millett, L.I. (eds.), *Engaging Privacy and Information Technology in a Digital Age*, National Academies Press, Washington, D.C. 2007. All references (including websites) in the present article are current as of 1st July 2010, and legislative references are to statutes in their amended form as of that date.

2 Conceptualisations of Privacy and Related Interests

The concept of privacy figures prominently in discourse about the social and political threats posed by modern information and communications technology (ICT). This is particularly so in the United States of America (U.S.A.), where "privacy" is a frequently used concept in public, academic and judicial discourse.[2] When serious discussion there took off in the 1960s about the implications of computerised processing of personal data, "privacy" was invoked as a key term for summing up the congeries of fears raised by the (mis)use of computers.[3] However, privacy has not been the only term invoked in this context. A variety of other, partly overlapping concepts have been invoked too, particularly those of "freedom", "liberty" and "autonomy".[4]

The U.S. debate, particularly in the 1960s and early 1970s, about the privacy-related threats posed by modern ICT exercised considerable influence on debates in other countries. As Hondius writes, "[a]lmost every issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale".[5] The salience of the privacy concept in U.S. discourse helped to ensure its prominence in the debate elsewhere. This is most evident in discourse in other English-speaking countries[6] and in international forums where English is a working language.[7] Yet also in countries in which English is not the main

2 *See* generally Regan, P.M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill / London 1995.

3 *See, e.g.,* Westin, A.F., *Privacy and Freedom*, Atheneum, New York 1970; Miller, A., *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Ann Arbor 1971.

4 The title of Westin's seminal work, *Privacy and Freedom*, *supra* note 3, is a case in point. Indeed, as pointed out further below, "privacy" in this context has tended to be conceived essentially as a form of autonomy – i.e., one's ability to control the flow of information about oneself.

5 Hondius, F.W., *Emerging Data Protection in Europe*, North Holland Publishing Company, Amsterdam 1975, p. 6. Even in more recent times, discourse in the U.S.A. often takes up such issues before they are discussed elsewhere. For example, systematic discussion about the impact of digital rights management systems (earlier termed "electronic copyright management systems") on privacy interests occurred first in the U.S.A.: *see* particularly Cohen, J.E., *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, Connecticut Law Review 1996, vol. 28, p. 981–1039. Similar discussion did not occur in Europe until a couple of years later – the first instance being Bygrave, L.A. and Koelman, K.J., *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems*, Institute for Information Law, Amsterdam 1998; later published in Hugenholtz, P.B. (ed.), *Copyright and Electronic Commerce*, Kluwer Law International, The Hague / London / New York 2000, p. 59–124.

6 *See, e.g.*, United Kingdom, Committee on Privacy (the Younger Committee), *Report of the Committee on Privacy*, Cm. 5012, Her Majesty's Stationery Office, London 1972; Canada, Department of Communications and Department of Justice, *Privacy and Computers: A Report of a Task Force*, Information Canada, Ottawa 1972; Australian Law Reform Commission, *Privacy*, Report no. 22, Australian Government Publishing Service, Canberra 1983; Morison, W.L., *Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General*, Report no. 170/1973, Australian Government Publishing Service, Canberra 1973.

7 As is evident, e.g., in the titles of the early Council of Europe resolutions dealing with ICT

language, much of the same discourse has been framed, at least initially, around concepts roughly equating with, or embracing, the notion of privacy – e.g., "la vie privée" (French),[8] "die Privatsphäre" (German),[9] "privatlivets fred" (Danish/Norwegian).[10]

Nevertheless, the field of law and policy which crystallised from the early European discussions on the privacy-related threats posed by ICT has often been described using a nomenclature that avoids explicit reference to "privacy" or closely related terms. This nomenclature is "data protection", deriving from the German term "Datenschutz".[11] While the nomenclature is problematic in several respects – not least because it fails to indicate the central interests served by the norms to which it is meant to apply[12] – it has gained broad popularity in Europe[13] and, to a lesser extent, elsewhere.[14] Its use, though, is being increasingly supplemented by the term "data privacy".[15] The latter nomenclature is arguably more appropriate than "data protection" as it better communicates the central interest(s) at stake and provides a bridge for synthesising North American and European policy discussions. However, it would be wrong to assume that the concepts of "data protection" and "privacy" are completely synonymous. While closely linked, they are not identical – at least from a European perspective. "Data protection" is typically reserved for a set of norms that serve a broader range of interests than simply privacy protection.[16] To the extent that those norms do engage with privacy protection, they focus only on the informational rather than spatial or physical dimensions of privacy.

---

threats. *See* Council of Europe Resolution (73)22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Private Sector (adopted 26th Sept. 1973); Council of Europe Resolution (74)29 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Public Sector (adopted 24th Sept. 1974).

8 *See, e.g.*, Messadie, G., *La fin de la vie privée*, Calmann-Levy, Paris 1974.

9 *See, e.g.*, the 1970 proposal by the (West) German Interparliamentary Working Committee for a "Gesetz zum Schutz der Privatsphäre gegen Missbrauch von Datenbankinformationen": described in Bull, H.P., *Datenschutz oder Die Angst vor dem Computer*, Piper, Munich 1984, p. 85.

10 *See, e.g.*, Denmark, Register Committee (Registerudvalget), *Delbetænkning om private registre*, Report no. 687, Statens trykningskontor, Copenhagen 1973.

11 Further on the origins of "Datenschutz", *see* Simitis, S. (ed.), *Bundesdatenschutzgesetz*, Nomos Verlagsgesellschaft, Baden-Baden 2006, 6th ed., p. 62–63.

12 Moreover, it has evidently tended to misleadingly connote, at least in U.S. circles, concern for security of data/information or maintenance of intellectual property rights: *see* Schwartz, P.M. and Reidenberg, J.R., *Data Privacy Law: A Study of United States Data Protection*, Michie Law Publishers, Charlottesville 1996, p. 5.

13 *See, e.g.*, Hondius, *supra* note 5.

14 *See, e.g.*, Hughes, G.L. and Jackson, M., *Hughes on Data Protection in Australia*, Law Book Co. Ltd., Sydney 2001, 2nd ed.

15 *See, e.g.*, Schwartz and Reidenberg, *supra* note 12; Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, Oxford 2003; and the title of the new journal, International Data Privacy Law, published by Oxford University Press from late 2010.

16 *See, e.g.*, Bygrave, L.A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague / London / New York 2002, chapter 7.

Moreover, as elaborated in section 5 below, data protection is increasingly being treated in European law as a set of rights that are separate to the more traditional right to respect for privacy or private life.

Various countries and regions display terminological idiosyncrasies that partly reflect differing jurisprudential backgrounds for the discussions concerned. In Western Europe, the discussion has often drawn upon jurisprudence developed there on legal protection of personality. Thus, the concepts of "Persönlichkeitsrecht" and "Persönlichkeitschutz" figure centrally in German and Swiss discourse on data protection.[17] Norwegian discourse revolves around the concept of "personvern" ("protection of person(ality)"),[18] while Swedish discourse focuses on "integritetsskydd" ("protection of (personal) integrity").[19] By contrast, Latin American discourse in the field tends to revolve around the concept of "habeas data" (roughly meaning "you should have the data"). This concept derives from due-process doctrine based on the writ of habeas corpus.[20]

Many of the above-mentioned concepts are prone to definitional instability. The most famous case in point is "privacy". Various definitions of the concept abound and a long – indeed, a long-winded – debate has raged, predominantly in U.S. circles, about which definition is most correct.[21] We find parallel debates in other countries which centre on similar concepts,[22] though these debates appear to be much less extensive than the privacy debate. Some of the latter debate concerns whether privacy as such is best characterised as a state/condition, a claim, or a right. That issue aside, the debate reveals four principal ways of

17 *See, e.g.,* Germany's Federal Data Protection Act of 1990 (*Bundesdatenschutzgesetz – Gesetz zum Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990*) (as amended) § 1(1) (stipulating the purpose of the Act as protection of the individual from interference with his/her "personality right" ("Persönlichkeitsrecht")); Switzerland's Federal Law on Data Protection of 1992 (*Loi fédérale du 19. juin 1992 sur la protection des données / Bundesgesetz vom 19. Juni 1992 über den Datenschutz*) Article 1 (stating the object of the Act as, *inter alia*, "protection of personality" ("Schutz der Persönlichkeit")).

18 *See* Bygrave, *supra* note 16, p. 138–143 and references cited therein.

19 *Ibid.*, p. 126–129 and references cited therein.

20 *See, e.g.,* Guadamuz, A., *Habeas Data: The Latin American Response to Data Protection*, The Journal of Information, Law and Technology 2000, no. 2, "www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz"; Organization of American States (O.A.S.), Inter-American Juridical Committee (rapporteur Fried, J.T.), *Right to Information: Access to and Protection of Information and Personal Data in Electronic Form*, in Annual Report of the Inter-American Juridical Committee, CJI/doc. 45/00, p. 107 *et seq*. While the concept originates in South America, it has also begun to gain a foothold in parts of South-East Asia. In 2008, the Supreme Court of the Philippines formally adopted a "Rule on the Writ of Habeas Data" as a Rule of Court.

21 For useful overviews, *see* Solove, D., *Understanding Privacy*, Harvard University Press, Cambridge, Massachusetts 2008, chapters 1–2; Inness, J.C., *Privacy, Intimacy, and Isolation*, Oxford University Press, New York / Oxford 1992, chapter 2; DeCew, J.W., *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, Ithaca / London 1997, chapters 2–3.

22 *See, e.g., En ny datalag*, Statens Offentliga Utredningar 1993, no. 10, p. 150–161 (documenting difficulties experienced in Swedish data protection discourse with respect to arriving at a precise definition of "personlig integritet").

defining privacy.[23] One set of definitions is in terms of *non-interference*,[24] another in terms of *limited accessibility*.[25] A third set of definitions conceives of privacy as *information control*.[26] A fourth set of definitions incorporates various elements of the other three sets but links privacy exclusively to *intimate* or *sensitive* aspects of persons' lives.[27]

Not surprisingly, definitions of privacy in terms of information control tend to be most popular in discourse dealing directly with law and policy on data protection.[28] The notion of information control informs much of that discourse both in the U.S.A. and elsewhere. In Europe, though, the notion is not always linked directly to the privacy concept; it is either linked to related concepts, such as "personal integrity" (in the case of, e.g., Swedish discourse),[29] or it stands alone. The most significant instance of the latter is the German notion of "information self-determination" ("informationelle Selbstbestimmung") which in itself forms the content of a constitutional right deriving from a landmark decision in 1983 by the German Federal Constitutional Court (Bundesverfassungsgericht).[30] The notion and the right to which it attaches, have had considerable impact on development of data protection law and policy in Germany[31] and, to a lesser extent, other European countries.

Despite the general popularity of notions of information control and information self-determination, these have usually not been viewed in terms of a person "owning" information about him-/herself, such that he/she should be entitled to, e.g., royalties for the use of that information by others.

---

23 *See* Bygrave, *supra* note 16, p. 128–129.

24 *See, e.g.*, Warren, S.D. and Brandeis, L.D., *The Right to Privacy*, Harvard Law Review 1890, vol. 4, p. 193, 205 (arguing that the right to privacy in Anglo-American law is part and parcel of a right "to be let alone").

25 *See, e.g.*, Gavison, R., *Privacy and the Limits of Law*, Yale Law Journal 1980, vol. 89, p. 421, 428–436 (claiming that privacy is a condition of "limited accessibility" consisting of three elements: "secrecy" ("the extent to which we are known to others"), "solitude" ("the extent to which others have physical access to us"), and "anonymity" ("the extent to which we are the subject of others' attention").

26 *See, e.g.*, Westin, *supra* note 3, p. 7 ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

27 *See, e.g.*, Inness, *supra* note 21, p. 140 (defining privacy as "the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions").

28 *See* generally Bygrave, *supra* note 16, p. 130 and references cited therein.

29 *See, e.g.*, *En ny datalag*, Statens Offentlige Utredningar 1993, no. 10, p. 159 (noting that the concept of "personlig integritet" embraces information control).

30 Decision of 15th December 1983, BverfGE (*Entscheidungen des Bundesverfassungsgerichts*), vol. 65, p. 1 *et seq*. For an English translation, *see* Human Rights Law Journal 1984, vol. 5, p. 94 *et seq*.

31 *Cf.* Simitis, S., *Das Volkzählungsurteil oder der lange Weg zur Informationsaskese – (BVerfGE 65, 1)*, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 2000, vol. 83, p. 359–375 (detailing the slow and incomplete implementation of the principles inherent in the right).

Concomitantly, property rights doctrines have rarely been championed as providing a desirable basis for data protection rules.[32] The relatively few proponents of a property rights approach have tended to come from the U.S.A.,[33] though sporadic advocacy of such an approach also occurs elsewhere.[34]

3 Conceptualisations of the Values Served by Privacy

How do various nations or cultures define the values promoted by respect for privacy? For instance, is privacy regarded as being mainly (or exclusively) of value to individual persons or is it also seen as having broader societal benefits?

In the U.S.A., most discourse on privacy and privacy rights tends to focus only on the benefits these have for individuals *qua* individuals. These benefits are typically cast in terms of securing (or helping to secure) *individuality*, *autonomy*, *dignity*, *emotional release*, *self-evaluation*, and inter-personal relationships of *love*, *friendship* and *trust*.[35] They are, in the words of Westin, largely about "achieving individual goals of self-realization".[36] The converse side of this focus is that privacy and privacy rights are often seen as essentially in tension with the needs of wider "society".[37] This view carries sometimes over into claims that privacy rights can be detrimental to societal needs.[38]

---

32 Opposition to a property rights approach is expressed in, *e.g.*, Miller, *supra* note 3, p. 211; Hondius, *supra* note 5, pp. 103–105; Simitis, S., *Reviewing Privacy in an Information Society*, University of Pennsylvania Law Review 1987, vol. 135, p. 707, 735–736; Wilson, K., *Technologies of Control: The New Interactive Media for the Home*, University of Wisconsin Press, Madison 1988, p. 91–94; Wacks, R., *Personal Information: Privacy and the Law*, Clarendon Press, Oxford 1989, p. 49; Poullet, Y., *Data Protection between Property and Liberties – A Civil Law Approach*, in Kaspersen, H.W.K. and Oskamp, A. (eds.), Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe, Kluwer Law & Taxation Publishers, Deventer / Boston 1990, p. 161–181; Litman, J., *Information Privacy/Information Property*, Stanford Law Review 2000, vol. 52, p. 1283–1313.

33 *See, e.g.*, Westin, *supra* note 3, p. 324–325; Laudon, K.C., *Markets and Privacy*, Communications of the Association for Computing Machinery 1996, vol. 39, p. 92–104; Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York 1999, p. 159–162; Rule, J.B. and Hunter, L., *Towards Property Rights in Personal Data*, in Bennett, C.J. and Grant, R. (eds.), Visions of Privacy: Policy Choices for the Digital Age, University of Toronto Press, Toronto 1999, p. 168–181; Rule, J.B., *Privacy in Peril*, Oxford University Press, Oxford 2007, p. 196–198. Cf. Schwartz, P.M., *Property, Privacy, and Personal Data*, Harvard Law Review, 2004, vol. 117, p. 2056–2128 (critically discussing various objections to a property approach but ultimately arguing in favour of a qualified "propertization" of personal data).

34 *See, e.g.*, Blume, P., *New Technologies and Human Rights: Data Protection, Privacy and the Information Society*, Paper no. 67, Institute of Legal Science, Section B, University of Copenhagen 1998.

35 *See* Bygrave, *supra* note 16, p. 133–134 and references cited therein.

36 Westin, *supra* note 3, p. 39.

37 *See* Regan, *supra* note 2, chapters 2, 8 and references cited therein.

38 As exemplified in Posner, R.A., *The Right to Privacy*, Georgia Law Review 1978, vol. 12, p. 393–422 (criticising privacy rights from an economic perspective) and Etzioni, A., *The*

Casting the value of privacy in strictly individualistic terms appears to be a common trait in the equivalent discourse in many other countries.[39] Indeed, it is an integral feature of what Bennett and Raab term the "privacy paradigm" – a set of liberal assumptions informing the development of data protection policy in the bulk of advanced industrial states.[40]

This notwithstanding, the grip of that paradigm varies from country to country and culture to culture. The variation is well exemplified when comparing the jurisprudence of the German Federal Constitutional Court with that of U.S. courts. The former emphasises that the value of data protection norms lies to a large degree in their ability to secure the necessary conditions for active citizen participation in public life; in other words, to secure a flourishing democracy.[41] This perspective is under-developed in U.S. jurisprudence.[42]

We find also increasing recognition in *academic* discourse on both sides of the Atlantic that privacy and data protection norms are valuable not simply for individual persons but for the maintenance of societal civility, pluralism and democracy.[43]

A related development is increasing academic recognition that data protection laws serve a multiplicity of interests that in some cases extend well beyond traditional conceptualisations of privacy.[44] This insight is perhaps furthest developed in Norwegian discourse, which has elaborated relatively sophisticated models of the various interests promoted by data protection laws.[45] These interests include ensuring adequate quality of personal information, "citizen-

---

Limits of Privacy, Basic Books, New York 1999 (criticising privacy rights from a communitarian perspective).

39 *See* Bennett, C.J. and Raab, C.D., *The Governance of Privacy. Policy Instruments in Global Perspective*, M.I.T. Press, Cambridge, Massachusetts 2006, 2nd ed., chapt. 1.

40 *Ibid.*

41 *See* especially the decision of 15th December 1983, *supra* note 30.

42 *See, e.g.*, Schwartz, P.M., *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, American Journal of Comparative Law 1989, vol. 37, p. 675–701; Ruiz, B.R., *Privacy in Telecommunications: A European and an American Approach*, Kluwer Law International, The Hague / London / Boston 1997; Eberle, E.J., *Dignity and Liberty: Constitutional Visions in Germany and the United States*, Praeger, Westport, Connecticut 2002, p. 88–94.

43 *See, e.g.*, Simitis, S., *Auf dem Weg zu einem neuen Datenschutzrecht*, Informatica e diritto 1984, p. 97–116; Post, R.C., *The Social Foundations of Privacy: Community and Self in the Common Law*, California Law Review 1989, vol. 77, p. 957–1010; Gavison, R., *Too Early for a Requiem: Warren and Brandeis were Right on Privacy vs. Free Speech*, South Carolina Law Review 1992, vol. 43, p. 437–471; Regan, *supra* note 2; Ruiz, *supra* note 41; Schwartz, P.M., *Privacy and Democracy in Cyberspace*, Vanderbilt Law Review 1999, vol. 52, p. 1609–1702; Bygrave, *supra* note 16; Bennett and Raab, *supra* note 39; Solove, *supra* note 21, 89 *et seq*.

44 *See, e.g.*, Mallmann, O., *Zielfunktionen des Datenschutzes: Schutz der Privatsphäre, korrekte Information; mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen*, Alfred Metzner Verlag, Frankfurt am Main 1977; Burkert, H., *Data-Protection Legislation and the Modernization of Public Administration*, International Review of Administrative Sciences 1996, vol. 62, p. 557–567; Bygrave, *supra* note 16, chapt. 7.

45 *See* Bygrave, *supra* note 16, p. 137 *et seq.* and references cited therein.

friendly" administration, proportionality of control, and rule of law. In Norway, the insight that data protection laws are concerned with more than safeguarding privacy, extends beyond the academic community and into regulatory bodies. Indeed, Norway's principal legislation on point contains an objects clause specifically referring to the need for "adequate quality of personal information" ("tilstrekkelig kvalitet på personopplysninger") in addition to the needs for privacy and personal integrity.[46]

The equivalent laws of some other European countries also contain objects clauses embracing more than privacy. The broadest, if not boldest, expression of aims is found in the French legislation: "Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties".[47]

Also noteworthy is the express concern in the early data protection legislation of several German *Länder* for maintaining State order based on the principle of separation of powers, and, concomitantly, for ensuring so-called "information equilibrium" ("Informationsgleichgewicht") between the legislature and other State organs. This "equilibrium" refers principally to a situation in which the legislature is able to get access to information (personal and/or non-personal) that is available to the executive.[48]

However, considerable uncertainty has reigned in many countries about exactly which interests and values are promoted by data protection laws. This is reflected partly in academic discourse,[49] partly in the fact that some of the laws lack objects clauses formally specifying particular interests or values which the legislation is intended to serve,[50] and partly in the vague way in which existing objects clauses are often formulated.[51]

---

46 *See* Personal Data Act of 2000 (*Lov om behandling av personopplysninger av 14. april 2000 nr. 31*), § 1(2).

47 *See* Act on Data Processing, Data Files and Individual Liberties of 1978 (*Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), Article 1.

48 *See* further Bygrave, *supra* note 16, p. 39; Simitis, *supra* note 11, p. 69.

49 *See, e.g.*, Korff, D., *Study on the Protection of the Rights and Interests of Legal Persons with regard to the Processing of Personal Data relating to such Persons*, final report to European Commission, October 1998, available via "ec.europa.eu/justice_home/fsj/privacy/studies/legal-persons_en.htm", p. 42 ("[t]here is a lack of clarity, of focus, over the very nature, aims and objects of data protection in the [European Union] Member States which is, not surprisingly, reflected in the international data protection instruments"); Napier, B.W., *International Data Protection Standards and British Experience*, Informatica e diritto 1992, p. 83, 85 (claiming that, in Britain, "the conceptual basis for data protection laws remains unclear").

50 *See, e.g.*, the U.K. Data Protection Act of 1998 and Denmark's Personal Data Act of 2000 (*Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger*).

51 *See, e.g.*, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series No. 108; adopted 28th Jan. 1981), Article 1 (specifying its goals as the protection of "rights and fundamental freedoms, and in particular … right to privacy").

4 Societal and Cultural Support for Privacy

Making accurate comparisons of the degree to which given countries or cultures respect privacy is fraught with difficulty – a problem that obviously carries over into comparative assessment of various countries' legal regimes for privacy and data protection.[52] Such difficulty is partly due to paucity of systematically collected empirical data,[53] and partly to the fact that concern for privacy within each country or culture is often uneven. In the United Kingdom (U.K.), for example, proposals to introduce multi-purpose Personal Identification Number (P.I.N.) schemes similar to those in Scandinavia[54] have traditionally been met with great antipathy, yet video surveillance of public places in the U.K. seems to be considerably more extensive than in Scandinavian countries and, indeed, the rest of the world.[55]

Levels of privacy across nations and cultures, and across broad historical periods, are in constant flux. Moreover, the ways in which human beings create, safeguard and enhance their respective states of privacy, and the extent to which they exhibit a desire for privacy, vary from culture to culture according to a complex array of factors.[56] At the same time, desire for some level of privacy appears to be a panhuman trait. Even in societies in which apparently little opportunity exists for physical or spatial solitude, human beings seem to adopt various strategies for cultivating other forms of social distance.[57]

---

52 Equally problematic, of course, is the accurate comparison of privacy levels across historical periods. As Bennett notes, "there is no one trajectory by which we can measure the progress or regress of privacy protection at any one time": Bennett, C.J., *The Privacy Advocates: Resisting the Spread of Surveillance*, M.I.T. Press, Cambridge, Massachusetts 2008), p. 221. *See* too Bennett and Raab, *supra* note 39, particularly p. 295. Yet another issue, over which relatively little has been written, concerns discrepancies between various classes of persons within a given society in terms of the respective levels of privacy they typically enjoy. For further discussion, *see* Bennett and Raab, *supra* note 39, chapt. 2.

53 As Bennett and Raab (*supra* note 39, p. 6) remark, "[u]nfortunately, we have little systematic cross-national survey evidence about attitudes to privacy with which to investigate the nature and influence of wider cultural attributes. Much of th[e] argumentation tends, therefore, to invoke anecdotes or cultural stereotypes: 'the Englishman's home is his castle', and so on".

54 Further on the Scandinavian P.I.N. schemes, *see, e.g.*, Lunde, A.S., Huebner, J., Lettenstrom, G.S., Lundeborg, S., Thygesen, L., *The Person-Number Systems of Sweden, Norway, Denmark and Israel*, U.S. Department of Health and Human Services; Vital and Health Statistics : Series 2 ; no. 84; D.H.H.S. Publication No. (P.H.S.) 80-1358, Washington, D.C. 1980.

55 Further on this surveillance, *see, e.g.*, *Der Spiegel*, 5th July 1999, p. 122–124; U.K. House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Second Report of Session 2008–09, H.L. Paper 18–I, H.M.S.O., London 2009, p. 20 and references cited therein. For a comparative discussion of U.K. and Norwegian video surveillance practices, see Lomell, H.M., *Selektive overblikk: En studie av videoovervåkingspraksis*, Universitetsforlaget, Oslo 2007, especially chapter 1.

56 *See, e.g.*, Moore, B., *Privacy: Studies in Social and Cultural History*, M.E. Sharpe, New York 1984; Roberts, J.M. and Gregor, T., *Privacy: A Cultural View*, in Pennock, J.R. and Chapman, J.W. (eds.), Privacy: Nomos XIII, Atherton Press, New York 1971, p. 199–225; Altman, I., *Privacy Regulation: Culturally Universal or Culturally Specific?*, Journal of Social Issues 1977, vol. 33, p. 66–84.

57 *See, e.g.*, Moore's study (*supra* note 56) of the Siriono Indians in Bolivia; and Flaherty's

To the extent that a panhuman *need* for privacy exists, this appears to be rooted not so much in physiological or biological but social factors. According to Moore, the need for privacy is, in essence, socially created. Moore's seminal study indicates that an extensive, highly developed concern for privacy is only possible in a relatively complex society with a strongly felt division between a domestic private realm and public sphere – "privacy is minimal where technology and social organization are minimal".[58]

However, technological-organizational factors are not the sole determinants of privacy levels. Also determinative are cultural, religious and philosophical factors. Central amongst these are attitudes to the value of private life,[59] attitudes to the worth of persons as individuals,[60] and sensitivity to human beings' non-economic and emotional needs.[61] Concern for privacy tends to be high in societies espousing liberal ideals, particularly those of Mill, Locke, Constant and Madison. As Lukes notes, privacy in the sense of a "sphere of thought and action that should be free from 'public' interference" constitutes "perhaps the central idea of liberalism".[62]

---

study of colonial society in New England (Flaherty, D.H., *Privacy in Colonial New England*, University Press of Virginia, Charlottesville 1972).

58 Moore, *supra* note 56, p. 276. *Cf.*, *inter alia*, Lunheim, R. and Sindre, G., *Privacy and Computing: A Cultural Perspective*, in Sizer, R., Yngström, L., Kaspersen, H., Fischer-Hübner, S. (eds.), Security and Control of Information Technology in Society, North-Holland, Amsterdam 1994, p. 25, 28 ("privacy is a cultural construct encountered in virtually every society of some economic complexity"). For an incisive sociological analysis of historical changes in levels and types of privacy, *see* Shils, E., *Center and Periphery: Essays in Macrosociology*, University of Chicago Press, Chicago / London 1975, chapt. 18.

59 *See, e.g.*, Arendt, H., *The Human Condition*, University of Chicago Press, Chicago 1958, p. 38 (noting that, in ancient Athenian culture, the private sphere was often regarded as a domain of "privation"). *See* also Moore, *supra* note 56, p. 120 *et seq.* Moore, however, discerns growing enthusiasm and respect for private life amongst Athenians over the course of the fourth century B.C.: *ibid.*, p. 128–133. *Cf.* Lü, Y.-H., *Privacy and data privacy issues in contemporary China*, Ethics and Information Technology, 2005, vol. 7, p. 7, 8 (noting that, in China, privacy has commonly been linked to the notion of *Yinsi*, which connotes a shameful secret).

60 *See, e.g.*, Schoeman, F.D., *Privacy and Social Freedom*, Cambridge University Press, Cambridge 1992, chapters 6–7 (describing factors behind the emergence of individualism and a concomitant concern for privacy in Western societies); Nakada, M. and Tamura, T., *Japanese conceptions of privacy: An intercultural perspective*, Ethics and Information Technology, 2005, vol. 7, p. 27, 29, 31 (explaining the relative lack of importance traditionally accorded in Japanese society to privacy as partly due to emphasis there on self-denial (*Musi*)); Kitiyadisai, K., *Privacy rights and protection: foreign values in modern Thai context*, Ethics and Information Technology, 2005, vol. 7, p. 17–26 (describing the misfit between the individualistic, Western concept of privacy on the one hand and, on the other, the collectivist character of traditional Thai culture and the lack of support in Buddhism for cultivating individualistic human rights).

61 *See, e.g.*, Strömholm, S., *Right of Privacy and Rights of the Personality: A Comparative Survey*, P.A. Norstedt & Söners Förlag, Stockholm 1967, p. 19–20 (viewing the development of legal rights to privacy as part and parcel of a "humanisation" of Western law; i.e., a trend towards greater legal sensitivity to the non-pecuniary interests of human beings).

62 Lukes, S., *Individualism*, Blackwell, Oxford 1973, p. 62.

The liberal affection for privacy is amply demonstrated in the development of legal regimes for privacy protection. These regimes are most comprehensive in Western liberal democracies – as shown in section 5 below. By contrast, such regimes are under-developed in most African and Asian nations. It is tempting to view this situation as symptomatic of a propensity in African and Asian cultures to place primary value on securing the interests and loyalties of the group at the expense of the individual. However, care must be taken not to paint countries and cultures into static categories. As elaborated in section 5 below, provision for privacy and data protection rights is increasingly on the legislative agenda of Asian and African countries.

Moreover, it should be kept in mind that, in the U.S.A. – often portrayed as the citadel of liberal ideals – legal protection of personal data falls short in significant respects of the protection levels in many other countries, especially the member states of the European Union (E.U.). The most glaring manifestation of this shortfall is the absence of comprehensive data protection legislation regulating the U.S. private sector and of an independent agency ("data protection authority" or "privacy commissioner") at the federal level to specifically oversee regulation of data protection matters.[63] Thus, within the Western liberal democratic "camp", considerable variation exists in legal regimes and readiness for safeguarding privacy – as shown further in section 5.

This variation, though, need not reflect differences between countries' respective levels of support for privacy. It can be attributable – at least in part – to differences in the extent to which persons in respective countries can take for granted that others will respect their privacy (independently of legal norms).[64] In other words, it can be attributable to differences in perceptions of the degree to which privacy is or will be threatened. For instance, the comprehensive, bureaucratic nature of data protection regulation in Europe[65] undoubtedly reflects traumas from relatively recent, first-hand experience there of totalitarian oppression. This heritage imparts both gravity and anxiety to European regulatory policy. Conversely, in North America and Australia, for example, the paucity of first-hand domestic experience of totalitarian oppression – at least for the bulk of "white society" – tends to make these countries' regulatory policy in the field relatively lax.

---

63 *See* also section 5.2. Further on the differences between U.S. and European regulatory approaches in the data protection field, *see, e.g.*, Charlesworth, A., *Clash of the Data Titans? US and EU Data protection Regulation*, European Public Law 2000, vol. 6, p. 253–274; Reidenberg, J.R., *Resolving Conflicting International Data protection Rules in Cyberspace*, Stanford Law Review 2000, vol. 52, p. 1315, 1330 *et seq*.; Whitman, J.Q., *The Two Western Cultures of Privacy: Dignity versus Liberty*, Yale Law Journal, 2004, vol. 113, p. 1151–1221.

64 It is claimed, for instance, that this difference accounts for the lack of judicial support in the U.K. for a tort of breach of privacy, in contrast to the willingness of U.S. courts to develop such a tort: *see, e.g.*, Martin, J. and Norman, A.R.D., *The Computerized Society*, Englewood Cliffs, New Jersey 1970, p. 468. However, other explanations have also been advanced for the non-development of a right to privacy in English common law: *see, e.g.*, Napier, *supra* note 49, p. 85 (emphasising the "narrow-mindedness" of English judges). For further detail on the divergent paths taken by English and American courts in developing a specific right of privacy under common law, *see, e.g.*, Tugendhat, M. and Christie, I. (eds.), *The Law of Privacy and The Media*, Oxford University Press, Oxford 2002, chapts. 2–3.

65 *See* section 5.2.

Variation between the privacy regimes of Western states can also be symptomatic of differences in perceptions of the degree to which interests that compete with privacy, such as public safety and national security, warrant protection at the expense of privacy interests. In other words, it can be symptomatic of differing perceptions of the need for surveillance and control measures. This is seen most clearly in the impact on U.S. regulatory policy of the terrorist attacks of 11th September 2001. In the wake of those attacks, the U.S. has been more prepared than before to curb domestic civil liberties, including privacy and data protection rights. As Regan observes, "[f]ollowing 9/11, discussions about information privacy in the United States have taken on a different character. Security worries trumped privacy concerns".[66]

Yet other factors can play a role too. For instance, U.S. and, to a lesser extent, Australian eschewal of "omnibus" data protection legislation for the private sector is due partly to distrust of State dirigism, combined with scepticism towards legally regulating the private sector except where there are proven to exist flagrant imbalances of power between private parties which cannot be corrected otherwise than by legislative intervention.[67]

The above differences aside, concern and support for privacy on the part of the general public seem to be broadly similar across the Western world.[68] There is abundant evidence from public opinion surveys that these levels of concern and support are relatively high,[69] at least in the abstract.[70] The concern for

66 Regan, P.M., *The United States*, in Rule, J.B. and Greenleaf, G. (eds.), Global Privacy Protection: The First Generation, Edward Elgar, Cheltenham 2008, p. 50, 67. For an overview of the post-9/11 inroads on privacy-related interests made by concerns about national security, particularly under the U.S. PATRIOT Act, *see ibid.*, p. 67–71.

67 With respect to U.S. attitudes, *see, e.g.*, Schwartz and Reidenberg, *supra* note 12, p. 6 *et seq.*; Regan, *supra* note 66, p. 74–76. Regan notes, though, that Americans' traditional distrust of government and relative trust of the private sector began to be "less compelling" in the late 1980s and 1990s, "[a]t least up until 9/11": *ibid.*, p. 76. For further analysis of the causes of divergence between Western countries' respective regimes for data protection, *see* Bennett, C.J., *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca 1992, chapt. 6.

68 As Bennett notes, "in nature and extent, the public concern for privacy is more striking for its cross-national similarities rather than for its differences": *ibid.*, p. 43.

69 *See, e.g.*, Bygrave, *supra* note 16, p. 110 and references cited therein; Bennett and Raab, *supra* note 39, p. 56–65 and references cited therein. The survey material referenced there derives mainly from the U.S.A., Canada, Australia, Norway, Denmark and the U.K. Survey material from Hungary seems largely to fit with the findings from the other countries: *see* Székely, I., *New Rights and Old Concerns: Information Privacy in Public Opinion and in the Press in Hungary*, Informatization and the Public Sector 1994, p. 99–113; Székely, I., *Hungary*, in Rule, J.B. and Greenleaf, G. (eds.), Global Privacy Protection: The First Generation, Edward Elgar, Cheltenham 2008, p. 174, 191 *et seq*. However, surveys of public attitudes to privacy can suffer from methodological weaknesses that make it unwise to rely upon their results as wholly accurate indications of public thinking: *see, e.g.*, Dutton, W.H. and Meadow, R.G., *A tolerance for surveillance: American public opinion concerning privacy and civil liberties*, in Levitan, K.B. (ed.), Government Infostructures, Greenwood Press, New York 1987, p. 167; Regan, *supra* note 66, p. 71.

70 Privacy concerns tend often to be of second-order significance for the public, with problems like public safety, unemployment and financial security being ranked as more important: *see, e.g.*, Bygrave, *supra* note 16, p. 110 and references cited therein.

privacy is often accompanied by considerable pessimism over existing levels of privacy, along with lack of trust that organisations will not misuse personal information.[71] Privacy concern tends to cut across a broad range of political leanings (within liberal democratic ideology),[72] though there are occasional indications of statistically significant variation in attitudes to privacy issues based on party-political attachments.[73] In terms of the roles played by other demographic variables, such as age, sex, and income level, results appear to vary from country to country and survey to survey.[74]

The survey evidence points to increasing public sensitivity to potential misuse of personal information. And one finds, for example, concrete instances where items of information that previously were routinely publicised are now subject to relatively stringent requirements of confidentiality.[75] Perhaps more interesting, however, is whether indications exist of an opposite development – i.e., increasing *acclimatisation* of people to situations in which they are required to divulge personal information and a concomitant adjustment of what they perceive as problematic for their privacy. For example, a commonplace assumption is that so-called "digital natives" – i.e., those born after 1980 who are immersed in the online world – are less concerned about privacy than are older generations. While this assumption is rooted in the obvious tendency of digital natives to disseminate a greater amount of information about themselves in online arenas than do older persons and is also supported by some reasonably reliable evidence,[76] other reliable evidence qualifies, if not undermines it.[77]

---

71 *Ibid.*, p. 111 and references cited therein.

72 *See* further Bennett, *supra* note 67, especially p. 147.

73 *See, e.g.*, Becker, H., *Bürger in der Modernen Informationsgesellschaft*, in Informations-gesellschaft oder Überwachungsstaat, Hessendienst der Staatskanzlei, Wiesbaden 1984, p. 343, 415–416 (citing survey results from (West) Germany showing that supporters of the Green Party (*Die Grünen*) were more likely to view data protection as important than were supporters of the more conservative political parties).

74 *Compare, e.g.*, Székely, *New Rights and Old Concerns*, *supra* note 69 (Hungarian survey results appear to show that demographic variables play little role in determining public attitudes to privacy issues) with Australian Federal Privacy Commissioner, *Community Attitudes to Privacy*, Information Paper 3, Australian Government Publishing Service, Canberra 1995 (demographic variables play significant role in Australian survey results).

75 *See, e.g.*, Torgersen, H., *Forskning og personvern*, in Blekeli, R.D. and Selmer, K.S. (eds.), Data og personvern, Universitetsforlaget, Oslo 1977, p. 223, 237 (noting that, in Norway, the quantity and detail of information publicly disclosed in connection with student matriculation were far greater in the 1960s than in the mid-1970s and onwards).

76 *See, e.g.*, Paine, C. *et al.*, *Internet users' perceptions of 'privacy concerns' and 'privacy actions'*, International Journal of Human-Computer Studies, 2007, vol. 65, p. 526–536 (presenting survey evidence indicating that older respondents – these came from around the world, with the largest groups coming from Russia (20 percent) and Germany (9 percent) – were more likely than younger respondents (i.e., those under 20 years of age) to be concerned about privacy in an online context); Teknologirådet, *Holdninger til personvern*, Teknologirådet, Oslo 2004 (documenting that Norwegian youths are less worried than older persons about the consequences of personal data misuse).

77 *See, e.g.*, Lenhart, A. and Madden, M., *Teens, Privacy and Online Social Networks*, Pew Research Center, Washington, D.C. 2007, "www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx" (presenting survey evidence indicating that many

Unfortunately, there seems otherwise to be little solid survey evidence addressing other aspects of the "acclimatisation" issue.

Public concern for privacy has rarely resulted in mass political movements with privacy and data protection *per se* high on their agenda. In the words of Bennett, "[t]here is no concerted worldwide privacy movement that has anything like the scale, resources or public recognition of organizations in the environmental, feminist, consumer protection, and human rights fields".[78] In most Western countries and, even more so, on the international plane, actual formulation of law and policy on data protection has typically been the project of a small elite.[79] It is tempting to draw a parallel between this state of affairs and the way in which privacy concerns were articulated and politically pushed in the 19th century, at least in the U.S.A. and Germany. The movement for legal recognition of privacy rights then and there had largely genteel, elitist traits – as embodied in the Massachusetts "Mugwump" movement of the 1880s. It was, as Westin observes, "essentially a protest by spokesmen for patrician values against the rise of the political and cultural values of 'mass society'".[80] This would be, however, an inaccurate (and unfair) characterisation of the modern "data protection elite". The agenda of the latter is strongly democratic and egalitarian; it is much more concerned about the welfare of the *citoyen* than simply that of the *bourgeois*. And it consciously draws much of its power from the privacy concerns of the general public.[81]

5 Regulatory Policy on Data Protection

This section provides an overview of the main legal instruments at both international and national levels which deal directly with data protection. Some

---

American teenagers care about their privacy and take a variety of measures to safeguard it in an online context); Paine *et al.*, *supra* note 76 (reporting that approximately 45 percent of respondents aged under 20 were concerned about privacy online; this figure climbed to approximately 60 percent for respondents aged 21–30 years).

78 *See* Bennett, *supra* note 52, p. 199. *See* also generally Bennett, *supra* note 67, p. 146, 243. *See* too Regan, *supra* note 66, p. 71 (observing in the context of U.S. public opinion that privacy concern tends to be latent rather than aggressive: "Privacy appears to be one of those low level concerns that do not mobilize people to anger or action").

79 *See* Bennett, *supra* note 67, p. 127 *et seq*. *See* too Bygrave, L.A., *International agreements to protect personal data*, in Rule, J.B. and Greenleaf, G. (eds.), Global Privacy Protection: The First Generation, Edward Elgar, Cheltenham 2008, p. 15, 17–19 (outlining the variety of actors who have contributed to the development of international privacy and data protection policy).

80 Westin, *supra* note 3, p. 348–349. *See* further Barron, J.H., *Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation*, Suffolk University Law Review 1979, vol. 13, p. 875–922; Howe, D.W., *Victorian Culture in America*, in Howe, D.W. (ed.), Victorian America, University of Pennsylvania Press, Philadelphia 1976, p. 3–28. For a similar critique with respect to the ideological and class roots of German "Persönlichkeitsrecht", see Schwerdtner, P., *Das Persönlichkeitsrecht in der deutschen Zivilordnung*, J. Schweitzer Verlag, Berlin 1977, especially p. 7, 85, 92.

81 *See* also Bennett, *supra* note 67, p. 129.

account is also taken of instruments which formally are not legally binding but are, nevertheless, highly influential in development of regulatory policy in the field.

The legal systems of many, if not most, countries contain a variety of rules which embody elements of the basic principles typically found in data protection instruments or which can otherwise promote these principles' realisation albeit in incidental, ad hoc ways. Rules concerning computer security, breach of confidence, defamation and intellectual property are examples. However, what is primarily of interest in the following overview is the degree to which countries have adopted rule-sets that are *directly* concerned with promoting data protection. Also of primary interest is the degree to which countries provide for the establishment of independent agencies (hereinafter termed "data protection authorities") specifically charged with overseeing the implementation and/or further development of these rule-sets.

5.1 International Instruments

The formal normative basis for data protection laws derives mainly from catalogues of fundamental human rights set out in certain multilateral instruments, notably the Universal Declaration of Human Rights (U.D.H.R.),[82] the International Covenant on Civil and Political Rights (I.C.C.P.R.)[83] along with the main regional human rights treaties, such as the European Convention on Human Rights and Fundamental Freedoms (E.C.H.R.)[84] and the American Convention on Human Rights (A.C.H.R.).[85] All of these instruments – with the exception of the African Charter on Human and People's Rights[86] – expressly recognise privacy as a fundamental human right.[87] The omission of privacy in the African Charter is not repeated in all human rights catalogues from outside the Western, liberal-democratic sphere. For example, the Cairo Declaration on Human Rights in Islam[88] expressly recognises a right to privacy for individuals (see Article 18(b) – (c)).

The right to privacy in these instruments is closely linked to the ideals and principles of data protection laws, though other human rights, such as freedom from discrimination and freedom of expression, are relevant too. The special importance of the right to privacy in this context is reflected in the fact that data protection laws frequently single out protection of that right as central to their

82 United Nations (U.N.) General Assembly resolution 217 A (III) of 10th Dec. 1948.

83 U.N. General Assembly resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March 1976.

84 European Treaty Series No. 5; opened for signature 4th Nov. 1950; in force 3rd Sept. 1953.

85 O.A.S. Treaty Series No. 36; adopted 22nd Nov. 1969; in force 18th July 1978.

86 O.A.U. Doc. CAB/LEG/67/3 rev. 5; adopted 27th June 1981; in force 21st October 1986.

87 See U.D.H.R., Article 12; I.C.C.P.R., Article 17; E.C.H.R., Article 8; A.C.H.R., Article 11. *See* also Article V of the American Declaration of the Rights and Duties of Man (O.A.S. Resolution XXX; adopted 1948).

88 Adopted 5th Aug. 1990 (U.N. Doc. A/45/421/5/21797, p. 199).

formal rationale.[89] It is also reflected in case law developed pursuant to I.C.C.P.R. Article 17 and E.C.H.R. Article 8: both provisions have been authoritatively construed as requiring national implementation of the basic principles of data protection laws with respect to both the public and private sectors.[90] Indeed, these provisions function, in effect, as data protection instruments in themselves. However, case law has yet to apply them in ways that add significantly to the principles already found in other data protection laws, and, in some respects, the protection they are currently held to offer, falls short of the protection afforded by many of the latter instruments.[91]

In terms of other international legal instruments, there is no truly global convention or treaty dealing specifically with data protection. Calls for such an instrument are increasingly made,[92] and work is underway to draft an appropriate set of international rules on point.[93] Yet while there is clearly a need for a global legal approach in the field, there is, realistically, scant chance of, say, a U.N.-sponsored convention being adopted in the short term. The closest to such an instrument at present is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

89 *See, e.g.,* Article 1 of the Council of Europe Convention on data protection, *supra* note 51; Article 2 of Belgium's 1992 Act Concerning the Protection of Personal Privacy in Relation to the Processing of Personal Data (*Wet van 8. December 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerkung van persoonsgegevens / Loi du 8. décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*); preamble to (and title of) Australia's federal Privacy Act of 1988.

90 In relation to Article 17 of the I.C.C.P.R., *see* General Comment 16 issued by the Human Rights Committee on 23rd March 1988 (U.N. Doc. A/43/40, p. 180–183), paragraphs 7 & 10. In relation to Article 8 of the E.C.H.R., *see, e.g.*, the judgments of the European Court of Human Rights in *Klass v. Germany* (1978) Series A of the Publications of the European Court of Human Rights ("A"), 28; *Malone v. United Kingdom* (1984) A 82; *Leander v. Sweden* (1987) A 116; *Gaskin v. United Kingdom* (1989) A 160; *Kruslin v. France* (1990) A 176-A; *Niemitz v. Germany* (1992) A 251-B; *Amann v. Switzerland* (2000) 30 E.H.R.R. 843; *Von Hannover v. Germany*, (2004) 40 E.H.R.R. 1; *Copland v U.K.* (2007) 45 E.H.R.R. 37. Of these judgments, that in *Von Hannover* deserves special mention as it is so far the sole Article 8 case involving data-processing practices of the private sector and it confirms that a state may breach its obligations under Article 8 if it does not lay down data protection rules with respect to such practices. For analysis of the above case law, *see* further De Hert, P. and Gutwirth, S., *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in Gutwirth, S. *et al* (eds.), Reinventing Data Protection? Springer Science, 2009, p. 14–29; Bygrave, L.A., *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology 1998, vol. 6, p. 247–284.

91 For instance, the right of persons to gain access to information kept on them by others is more limited under Article 8 of the E.C.H.R. than is usual under ordinary data protection laws: *see, e.g.,* Bygrave, *supra* note 90, p. 277 *et seq*.

92 *See* further Kuner, C., *An international legal framework for data protection: Issues and prospects*, Computer Law & Security Review, 2009, vol. 25, p. 307–317 and references cited therein.

93 *E.g.,* draft international rules on the protection of data and privacy were presented at the 31st International Conference of Data Protection and Privacy Commissioners in Madrid November 2009.

(hereinafter "C.o.E. Convention").[94] Although this is a European instrument, it is envisaged to be potentially more than an agreement between European states as it is open to ratification by states not belonging to the Council of Europe, though only upon the Council's invitation (see Article 23). Civil society representatives have recently pushed to get non-member states to take advantage of this possibility,[95] though it is too early to tell whether this initiative will bear fruit. At present, the Convention has yet to be ratified by a non-member state.

As for the E.U., its constitutional instruments now recognise that protection of personal data is in itself (i.e., separate from the broader right to privacy) a basic human right.[96] This is a significant and hitherto unique development at the international level.

Additionally, the E.U. has adopted several Directives on data protection. The first and most important of these is Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (hereinafter "E.U. Directive").[97] This instrument is binding on E.U. member states, albeit with several qualifications, the most significant being that the Directive does not apply to activities relating to "public security, defence, State security ... and the activities of the State in areas of criminal law" (Article 3(2)).[98] At the same time, though, member states are free to subject such activities to data protection regimes modelled on the Directive. Certain non-member states (Norway, Iceland and Liechtenstein) that are party to the 1992 Agreement on the European Economic Area (E.E.A.) are also bound to implement the Directive, with the same qualifications as just noted.

---

94 European Treaty Series No. 108; adopted 28th Jan. 1981; in force 1st Oct. 1985. Further on the Convention, *see, e.g.*, Henke, F., *Die Datenschutzkonvention des Europarates*, Peter Lang, Frankfurt am Main / Bern / New York 1986; Bygrave, *supra* note 79, p. 19–26.

95 *See* Madrid Privacy Declaration: Global Privacy Standards for a Global World, 3rd Nov. 2009, "thepublicvoice.org/madrid-declaration/" (urging countries that have not yet ratified the Convention or its 2001 Protocol "to do so as expeditiously as possible").

96 *See* Charter of Fundamental Rights of the European Union, adopted 7th Dec. 2000 (O.J. C 364, 18th Dec. 2000, p. 1 *et seq.*), Article 8 (providing for a right to protection of personal data) and Article 7 (providing for the right to respect for private and family life). As of 1st December 2009, the Charter has been given the same legal value as the EU Treaties under Article 6(1) of the Treaty on European Union, as amended by the Treaty of Lisbon (adopted 13th Dec. 2007; in force 1st Dec. 2009; O.J. C 306, 17th Dec. 2007, p. 1 *et seq.*). This status of the Charter applies to all EU member states except for the U.K. and Poland. A specific right to data protection is also provided by Article 16 of the Treaty on the Functioning of the European Union (the new name given by the Lisbon Treaty to the Treaty establishing the European Community).

97 Adopted 24th Oct. 1995 (Official Journal of the European Communities (O.J.), L 281, 23rd Nov. 1995, p. 31 *et seq.*). Further on the Directive, *see, e.g.*, Bainbridge, D.I., *EC Data Protection Directive*, Butterworths, London / Dublin / Edinburgh 1996; Damman, U. and Simitis, S., *EG-Datenschutzrichtlinie: Kommentar*, Nomos Verlagsgesellschaft, Baden-Baden 1997.

98 *I.e.*, activities that used to fall within the ambit of the E.U.'s old "Third Pillar" and "Second Pillar" and, as such, outside the scope of the former European Community (the old "First Pillar"). The formal division of E.U. competence and activity manifest in the pillar system has been abolished with the coming into force of the Lisbon Treaty. Nonetheless, the effects of the system continue to mark the ambit of legal instruments that were a child of it – the Data Protection Directive being one such instrument.

While the Directive is primarily a European instrument for European states, it exercises considerable influence over other countries not least because it places a qualified prohibition on transfer of personal data to those countries unless they provide "adequate" levels of data protection (see Articles 25–26).[99] As shown below, many non-European countries are passing legislation in order, at least partly, to meet this adequacy criterion.[100] Furthermore, the Directive stipulates that the data protection law of an E.U. state may apply outside the E.U. in certain circumstances, most notably if a data controller,[101] based outside the E.U., utilises "equipment" located in the state to process personal data for purposes other than merely transmitting the data through that state (see Article 4(1)(c)).[102] All of these provisions give an impression that the E.U., in effect, is legislating for the world.[103]

Apart from the above legal instruments, there exist numerous international and regional instruments on data protection which take the form of guidelines, recommendations, or codes of practice. Although "soft law" only, some of them carry a great deal of political and/or commercial weight; accordingly, they exercise considerable influence on the development of data protection law. For advanced industrial states generally, the most significant of these instruments are the 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Organization for Economic Cooperation and Development (O.E.C.D.).[104] The Guidelines contain a set of data protection

99 Further on the Directive's restrictions on transborder data transfers, *see, e.g.,* Kuner, C., *European Data Protection Law: Corporate Compliance and Regulation*, Oxford University Press, Oxford 2007, 2nd rev. ed., chapter 4.

100 Further on this influence, *see, e.g.*, Newman, A.L., *Protectors of Privacy: Regulating Personal Data in the Global Economy*, Cornell University Press, Ithaca 2008, especially chapters 4–5; Swire, P.P. and Litan, R.E., *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, Washington, D.C. 1998; Shaffer, G., *Globalization and Social Protection: The Impact of E.U. and International Rules in Ratcheting Up of U.S. Privacy Standards*, Yale Journal of International Law 2000, vol. 25, p. 1–88; Waters, N., *The European influence on privacy law and practice*, Privacy Law & Policy Reporter 2003, vol. 9, p. 150–155.

101 A "data controller" is a person or organisation who/which determines the purposes and means of processing personal data: *see* E.U. Directive, Article 2(d).

102 *See* further Bygrave, L.A., *Determining Applicable Law pursuant to European Data Protection Legislation*, Computer Law & Security Report (now Review) 2000, vol. 16, p. 252–257; Kuner, *supra* note 99, chapter 3.

103 Equally, they nourish accusations of "regulatory overreaching". *See* particularly the criticism of Article 4(1)(c) in Bygrave, *supra* note 100. *See* also the more general criticism in, *e.g.*, Lukas, A., *Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive*, Trade Policy Analysis Paper no. 16, 30th Oct. 2001, Cato Institute, Washington, D.C. 2001; Ford, P., *Implementing the EC Directive on data protection – an outside perspective*, Privacy Law & Policy Reporter 2003, vol. 9, p. 141–149; Kuner, *supra* note 99, chapter 3; Kuner, C., *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, International Journal of Law and Information Technology, 2010, vol. 18 (forthcoming).

104 Adopted by O.E.C.D. Council on 23rd Sept. 1980 (O.E.C.D. Doc. C(80)58/FINAL). Further on the Guidelines, *see, e.g.*, Seipel, P., *Transborder Flows of Personal Data: Reflections on the OECD Guidelines*, Transnational Data Report 1981, vol. 4. p. 32–44.

principles similar to those stipulated in the C.o.E. Convention. The Guidelines have been very influential on the drafting of data protection laws and standards in non-European jurisdictions, such as Australia, New Zealand and Canada.[105] They have also been formally endorsed – though not necessarily implemented – by numerous companies and trade associations in the U.S.A.[106] Further, they constitute an important point of departure for the Privacy Framework adopted by the Asia Pacific Economic Cooperation (A.P.E.C.).[107] The core of that Framework is a set of "Information Privacy Principles" that are essentially somewhat diluted versions of the main principles of the O.E.C.D. Guidelines – hence, their apt description by one commentator as "OECD Lite".[108]

Of potentially broader reach are the United Nations (U.N.) Guidelines Concerning Computerized Personal Data Files (hereinafter "U.N. Guidelines"), adopted 1990.[109] The Guidelines are intended to encourage enactment of data

---

The O.E.C.D. has issued other guidelines also relating, albeit more indirectly, to data protection: *see* Guidelines for the Security of Information Systems (adopted 26th Nov. 1992) – now replaced by Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (adopted 25th July 2002); Guidelines for Cryptography Policy (adopted 27th March 1997); Guidelines for Consumer Protection in the Context of Electronic Commerce (adopted 9th Dec. 1999); and Guidelines on Human Biobanks and Genetic Research Databases (adopted 22nd October 2009). *See* too Declaration on the Protection of Privacy on Global Networks (C(98)177, Annex 1; issued 8–9th October 1998) and Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (adopted 12th June 2007).

105 Reference to the Guidelines is made in the preambles to both Australia's federal Privacy Act of 1988 and New Zealand's Privacy Act of 1993. Further on the Guidelines' importance for Australian policy, *see* Ford, *supra* note 103. In Canada, the Guidelines formed the basis for the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), adopted in March 1996. The Model Code has been incorporated into Canadian legislation as Schedule 1 to the Personal Information Protection and Electronic Documents Act of 2000.

106 *See, e.g.*, Gellman, R.M., *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, Software Law Journal 1993, vol. 6, p. 199, 230.

107 The A.P.E.C. states are Australia, Brunei, Canada, Chile, China, Hong Kong, China, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, the Russian Federation, Singapore, Taiwan, Thailand, the USA and Vietnam.

108 *See* Greenleaf, G., *Australia's APEC privacy initiative: the pros and cons of 'OECD Lite'*, Privacy Law & Policy Reporter, 2003, vol. 10, p. 1–6. *See* too Greenleaf, G., *APEC's privacy framework sets a new low standard for the Asia-Pacific*, in Kenyon, A.T. and Richardson, M. (eds.), New Dimensions in Privacy Law: International and Comparative Perspectives, Cambridge University Press, Cambridge 2005, p. 91–120. For other, less critical views of the A.P.E.C. initiative, *see, e.g.*, Waters, N., *The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a trojan horse for self-regulation?*, SCRIPTed, 2009, vol. 6, 75, "www.law.ed.ac.uk/ahrc/script-ed/vol6-1/waters.asp"; Tan, J.G., *A Comparative Study of the APEC Privacy Framework – A New Voice in the Data Protection Dialogue?*, Asian Journal of Comparative Law, 2008, vol. 3, issue 1, article 7, "www.bepress.com/asjcl/vol3/iss1/art7/".

109 On the background to the Guidelines, *see, e.g.*, Michael, J., *Privacy and Human Rights. An International and Comparative Study, with Special Reference to Developments in Information Technology*, UNESCO/Dartmouth Publishing Company, Paris / Aldershot 1994, p. 21–26.

protection laws in U.N. Member States lacking such legislation. The Guidelines are also aimed at encouraging international organisations – both governmental and non-governmental – to process personal data in a responsible, fair and privacy-friendly manner. However, the Guidelines seem to have had little practical effect relative to the O.E.C.D. Guidelines and the other instruments canvassed above.[110] Nevertheless, their adoption underlines that data protection is not simply a "First World", Western concern. Moreover, in several respects, the principles in the U.N. Guidelines go further than some of the other international instruments.[111]

Note should also be taken of the numerous codes, recommendations, etc. that are of sectoral application only. The C.o.E. has been the most active international actor in this regard, issuing a large range of sector-specific recommendations to supplement and extend the rules in its Convention on data protection. These recommendations cover, *inter alia*, the police sector,[112] employment,[113] research and statistics,[114] and telecommunications.[115] The International Labour Organization (I.L.O.) is another noteworthy actor, having adopted a code of practice on data protection in the workplace.[116]

As for the E.U., it has adopted several sectoral Directives on data protection. The first of these was Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.[117] This has been repealed and replaced by Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.[118] A controversial Directive on retention of communications traffic data was then passed in 2006, modifying the impact of Directive 2002/58/EC by requiring E.U. member states to ensure that providers of public communications networks store traffic data for a minimum of 6 months and maximum of 2 years.[119] Additionally, the E.U. has adopted a Regulation on

110 This is partly reflected in the fact that they are frequently overlooked in data protection discourse, at least in Scandinavia: *see* Bygrave, *supra* note 16, p. 33 and references cited therein.

111 For details, *see* Bygrave, *supra* note 16, p. 73, 350.

112 Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector (adopted 17th Sept. 1987).

113 Recommendation No. R (89) 2 on the Protection of Personal Data used for Employment Purposes (adopted 18th Jan. 1989).

114 Recommendation No. R (83) 10 on the Protection of Personal Data used for Scientific Research and Statistics (adopted 23rd Sept. 1983); Recommendation No. R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes (adopted 30th Sept. 1997).

115 Recommendation No. R (95) 4 on the Protection of Personal Data in the Area of Telecommunications Services, with Particular Reference to Telephone Services (adopted 7th Feb. 1995).

116 *Protection of Workers' Personal Data*, I.L.O., Geneva 1997.

117 Adopted 15th Dec. 1997 (O.J. L 24, 30th Jan. 1998, p. 1 *et seq.*).

118 Adopted 12th July 2002 (O.J. L 201, 31st July 2002, p. 37 et seq.).

119 *See* Directive 2006/24/EC of 15th March 2006 on the Retention of Data Generated or

data protection with regard to the data-processing practices of E.U. institutions,[120] and, rather "late in the day", a Framework Decision on data protection for the police sector.[121]

The principal international instruments dealing specifically with data protection tend to be aimed not just at encouraging enactment of national rules but also harmonisation of these rules. The harmonisation objective has, in turn, several rationales, some of which are not so much concerned with enhancing data protection as facilitating the flow of personal data across national borders in order to maintain international commerce, freedom of expression, and inter-government cooperation.[122] The latter concerns arise because many national data protection laws – mainly European – have long operated with rules providing for restrictions of data flow to countries not offering levels of data protection similar to the "exporting" jurisdiction.[123] While the practical effect of such rules on actual transborder data flow tends to have been, for the most part, negligible,[124] their potential impact has caused much consternation, particularly for business interests. Concern to minimise this impact in order to safeguard trade is most prominent in the O.E.C.D. Guidelines, A.P.E.C. Privacy Framework and E.U. Directive.[125] The latter goes the furthest in securing regional transborder data flow by prohibiting E.U. member states from instituting privacy-related restrictions on data transfer to other member states (see Article 1(2)). This prohibition is primarily grounded in the need to facilitate realisation of the E.U.'s internal market.[126] At the same time, however, the Directive goes the

---

Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC (O.J. L 105, 13th April 2006, p. 54–63).

120 Regulation (EC) 45/2001 of 18th Dec. 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Institutions and Bodies of the Community and on the Free Movement of such Data (O.J. L 8th Dec. 2001, p. 1 *et seq*.).

121 Council Framework Decision 2008/977/JHA of 27th Nov. 2008 on the Protection of Personal Data processed in the Framework of Police and Judicial Cooperation in Criminal Matters (O.J. L 350, 30th Dec. 2008, p. 60–71). It is important to note that this instrument does not cover domestic, intra-member state processing of personal data by police, only data that "are or have been transmitted or made available between Member States" (Article 1(2)(a)). The Decision is also "without prejudice to essential national security interests and specific intelligence activities in the field of national security" (Article 1(4)). For critical analyis of its background and aims, *see* De Hert, P. and Papakonstantinou, V., *The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement, however not the improvement some have hoped for*, Computer Law & Security Review, 2009, vol. 25, p. 403–14.

122 *See* generally Bygrave, *supra* note 16, p. 40 and references cited therein.

123 For details, *see, e.g.*, Nugter, A.C.M., *Transborder Flow of Personal Data within the EC*, Kluwer Law & Taxation Publishers, Deventer / Boston 1989; Ellger, R., *Der Datenschutz im grenzüberschreitende Datenverkehr: eine rechtsvergleichende und kollisionsrechtliche Untersuchung*, Nomos Verlagsgesellschaft, Baden-Baden 1990.

124 *See, e.g.*, the extensive survey in Ellger, *supra* note 123.

125 *See* Bygrave, *supra* note 16, p. 40 and references cited therein.

126 *See* particularly recitals 3, 5 and 7 in the preamble to the Directive.

furthest of the international instruments in restricting transborder data flow, through its qualified prohibition of data transfer to non-E.U. states that fail to provide "adequate" levels of data protection (Article 25).

The adequacy criterion could be regarded as evidence that economic protectionism forms part of the Directive's agenda – i.e., a desire to protect European industry from foreign competition. Allegations of economic protectionism have been directed at earlier European data protection regimes,[127] but little solid evidence exists to support them.[128] While there is perhaps more evidence linking the origins of the Directive to protectionist concerns, the linkage is still tenuous.[129] Considerably more solid grounds exist for viewing the adequacy criterion as *prima facie* indication that the Directive is seriously concerned with safeguarding privacy interests and rights. This concern is also manifest in the preamble to the Directive,[130] in case law from the E.U. Court of Justice,[131] and in the E.U.'s constitutional foundations, where, as noted above, protection of personal data is posited as a basic human right in itself.

Despite their harmonising objectives, the international instruments tend to leave countries a significant degree of leeway in development of their respective data protection regimes. This is especially the case with the "soft law" instruments. Yet also the legally binding instruments allow for considerable national flexibility. The C.o.E. Convention is not intended to be self-executing and permits derogations on significant points.[132] As for the E.U. Directive, while this has more prescriptive "bite" than its counterparts, it is still aimed only at facilitating an "approximation" as opposed to complete uniformity of national laws (see particularly recital 9 in its preamble). Accordingly, it leaves E.U. member states considerable margin for manoeuvre.[133]

Of all of the instruments canvassed above, the E.U. Directive has become the leading trendsetter and benchmark for data protection around the world. Not only is it shaping national data protection regimes, it is also shaping international instruments. For example, the C.o.E. Convention has been supplemented by a protocol containing rules that essentially duplicate the rules in the Directive dealing respectively with flow of personal data to non-member states and with the competence of national data protection authorities.[134] Outside Europe, clear

127 *See, e.g.*, Eger, J.M., *Emerging Restrictions on Transborder Data Flow: Privacy Protection or Non-Tariff Trade Barriers*, Law and Policy in International Business 1978, vol. 10, p. 1055–1103; Pinegar, K.R., *Privacy Protection Acts: Privacy Protectionism or Economic Protectionism?*, International Business Lawyer 1984, vol. 12, p. 183–188.

128 *See* Bygrave, *supra* note 16, p. 114–115 and references cited therein.

129 *Id.*

130 *See* particularly recitals 2, 3, 10 and 11.

131 *See, e.g.*, joined cases C-465/00, C-138/01, and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, particularly paragraphs 68 *et seq.*

132 *See* Henke, *supra* note 94, especially p. 57–60; Bygrave, *supra* note 16, p. 34.

133 *See* further Bygrave, *supra* note 16, p. 34 and references cited therein. *See* also section 5.3 below.

134 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder

traces of the Directive are to be found in, e.g., the data protection laws of Dubai, Malaysia and Macau,[135] and in draft data protection legislation being prepared in the Philippines.[136]

Nevertheless, the leadership status of the Directive faces challenge in the Asia Pacific region, particularly given that A.P.E.C. has been able to agree on a Privacy Framework for its 21 member states. As indicated above, the principles in that Framework are more inspired by the O.E.C.D. Guidelines than the Directive, at the same time as they are significantly less privacy-protective than the Directive (and arguably the Guidelines). The Framework signals a readiness amongst many of the A.P.E.C. states to forge their own approach to data protection without necessarily conforming to European norms. This approach appears to foster data protection regimes less because of concern to protect basic human rights than concern to engender consumer confidence in business.[137] However, the A.P.E.C. Privacy Framework has yet to have any substantial influence on the shape of national data protection laws in the region, relative to the influence that has hitherto been exercised by the Directive and the O.E.C.D. Guidelines.[138]

5.2 National Instruments

Well over forty countries have enacted data protection laws, and their number is growing steadily.[139] The bulk of these countries are European. Indeed, Europe is home to the oldest, most comprehensive and most bureaucratically cumbersome data protection laws at both national and provincial levels. Moreover, as shown

---

data flows (C.E.T.S. No. 181; adopted 23rd May 2001; in force 1st July 2004).

135 For Dubai, *see* Dubai International Financial Centre (DIFC) Law No. 1 of 2007. For Malaysia, *see* Personal Data Protection Act of 2010; for Macau, *see* Personal Data Protection Act of 2006. Further on Dubai's legislation, see Michael, J., *Dubai adopts first DP law in an Arab country*, Privacy Laws & Business International Newsletter, 2007, issue 86, p. 1, 3–5. Further on the Malaysian legislation, *see* Munir, A.B., *Malaysia introduces personal data protection bill*, Privacy Laws & Business International Newsletter, 2009, issue 102, p. 18–19; Greenleaf, G., *Malaysia passes DP bill*, Privacy Laws & Business International Newsletter, 2010, issue 104, p. 1, 5–7. Further on the Macau legislation, *see* Greenleaf, G., *Macau's EU-influenced Personal Data Protection Act*, Privacy Laws & Business International Newsletter, 2008, issue 96, p. 21–22.

136 *See* Parlade, C., *Philippines likely to adopt EU-style privacy and DP law*, Privacy Laws & Business International Newsletter, 2008, issue 95, p. 16–18.

137 *See, e.g.,* Tang, R., *Personal data protection: the Asian agenda*, speech given at 25th International Conference of Data Protection and Privacy Commissioners, Sydney, 10th Sept. 2003, available via "www.privacyconference2003.org/program.asp#psa"; Bygrave, *supra* note 79, p. 43–44.

138 *See* too Greenleaf, G., *Twenty-one years of Asia-Pacific data protection*, Privacy Laws & Business International Newsletter, 2009, issue 100, p. 21, 23 (noting that the influences on data protection principles in the Asia-Pacific region "are principally the OECD Guidelines and the EU Directive, but the APEC Privacy Framework has not yet had any direct influence. The influence of the EU Directive is, if anything, strengthening over time").

139 *See* generally Electronic Privacy Information Center (EPIC) and Privacy International (PI), *Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments*, EPIC / PI, Washington, D.C. 2006, which gives a fairly up-to-date overview of the state of data protection regimes in over 50 countries.

above, Europe – through its supranational institutions – is also springboard for the most ambitious and extensive international initiatives in the field.

Common points of departure for national data protection regimes in Europe are as follows:

- coverage of both public and private sectors;
- coverage of both automated and manual systems for processing personal data largely irrespective of how the data are structured;
- application of broad definitions of "personal data";
- application of extensive sets of procedural principles some of which are rarely found in data protection regimes elsewhere;[140]
- more stringent regulation of certain categories of sensitive data (e.g., data relating to philosophical beliefs, sexual preferences, ethnic origins);
- restrictions on transborder flow of personal data;
- establishment of independent data protection agencies with broad discretionary powers to oversee implementation and development of data protection rules;
- channelling of privacy complaints to these agencies rather than courts;
- extensive subjection of data processing to notification and/or licensing requirements administered by the data protection agencies;
- extensive use of "opt-in" requirements for valid consent by data subjects;
- little use of industry-developed codes of practice.[141]

While the bulk of these characteristics are typical for national data protection regimes in Europe, each country there has its own unique mix of rules; concomitantly, a good deal of variation exists in the degree to which each country shares the above-listed traits.[142] For example, the Netherlands has

140 An example of a principle that is rarely found other than in European laws concerns fully automated profiling. The principle is that fully automated assessments of a person's character should not form the sole basis of decisions that impinge upon the person's interests. The principle is embodied in Article 15 of the E.U. Directive: *see* further Bygrave, *supra* note 16, p. 319–328.

141 For further details, *see*, *e.g.*, Korff, D., *Data Protection Law in the European Union*, Direct Marketing Association / Federation of European Direct and Interactive Marketing, New York / Brussels 2005; Bygrave, *supra* note 16, chapts. 2–4; Kuner, *supra* note 99.

142 *See* generally Korff, D., *EC Study on Implementation of Data Protection Directive – Comparative summary of national laws*, report for European Commission, September 2002,

always made relatively extensive use of industry-based codes of practice, and the E.U. Directive itself encourages greater use of such codes (see Article 27). Moreover, data protection regimes in each country are far from static. For example, Swedish legislation originally operated with relatively extensive licensing and notification requirements; now it has dispensed entirely with a licensing scheme, cut back significantly on notification requirements and introduced "light-touch", misuse-oriented regulation for the processing of unstructured electronic data.[143] There has been movement too at a broader European level. For instance, while many early European data protection regimes relied heavily on paternalistic control mechanisms (i.e., control exercised by government bodies (primarily data protection agencies) on behalf and supposedly in the best interests of citizens (data subjects)), they now show greater readiness to rely more on participatory control (i.e., control exercised by citizens themselves), supplemented by greater readiness to embrace market mechanisms for regulation of data processing. This notwithstanding, European jurisdictions (in contrast to, say, the U.S.A.) generally still maintain a relatively non-negotiable legislative baseline for the private sector.

Across the Atlantic, Canada and Argentina come closest to embracing the European approach. Canada has federal legislation in place aimed at ensuring comprehensive protection of personal data in relation to both the public and private sectors.[144] All Canadian Provinces and Territories have also enacted data protection legislation in relation to provincial and territorial government agencies; the legislation of several provinces also covers the private sector.[145] Data protection agencies exist at both federal and provincial levels. The E.U. Commission (hereinafter "European Commission") has formally ruled that, in general, Canada offers "adequate" protection for personal data pursuant to Article 25 of the E.U. Directive.[146] As for Argentina, it enacted legislation in 2000 modelled on the E.U. Directive and equivalent Spanish legislation, and formally based on the right of *habeas data* provided in its Constitution (Article 43).[147] Like with Canada, the European Commission has formally ruled that Argentina satisfies the E.U. Directive's adequacy criterion.[148] Mexico might

---

available via "ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm".

143 *See* Personal Data Act of 1998 (*Personuppgiftslagen*, S.F.S 1998:204), sections 5a, 36–37. By "misuse-oriented" regulation is meant regulation that applies only insofar as the data processing in question violates the personal integrity of the data subject: *see* further *Översyn av personuppgiftslagen*, Statens Offentlige Utredningar 2004, no. 6.

144 *See* Privacy Act of 1982; Personal Information Protection and Electronic Documents Act of 2000.

145 S*ee, e.g.*, Quebec's Act on Protection of Personal Information in the Private Sector of 1993; British Columbia's Personal Information Protection Act of 2003; Alberta's Personal Information Protection Act of 2003 and Health Information Act of 1999.

146 Decision 2002/2/EC of 20th Dec. 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (O.J. L 2, 4th Jan. 2002, p. 13 *et seq.*).

147 *See* Law for the Protection of Personal Data of 2000.

148 Decision C(2003) 1731 of 30th June 2003 pursuant to Directive 95/46/EC of the European

well be joining this "adequacy" club in the not too distant future as it has fairly comprehensive data protection legislation in place for the public sector and similar legislation for the private sector was recently passed by the Mexican Senate.[149] It has also established a data protection authority (Federal Institute of Access to Information and Data Protection).

By contrast, European-style data protection authorities do not exist in the U.S.A. and its legal regime for data protection is relatively atomised. While there is quite extensive legislation dealing with federal government agencies,[150] omnibus legislative solutions are eschewed with respect to the private sector. Legal protection of data protection in relation to the latter takes the form of ad hoc, narrowly circumscribed, sector-specific legislation, combined with recourse to litigation based on the tort of invasion of privacy and/or breach of trade practices legislation.[151] At the same time, though, a "safe harbour" agreement has been concluded between the U.S.A. and E.U. allowing for the flow of personal data from the E.U. to U.S.-based companies that voluntarily agree to abide by a set of "fair information" principles based loosely on the E.U. Directive. Despite slow corporate take-up in its early days, the scheme now has over 2000 corporations (including major businesses) formally certifying adherence to it.[152] Although the European Commission has determined that the scheme satisfies the Directive's adequacy test in Article 25,[153] considerable evidence has since accrued to indicate significant shortcomings in the scheme's effectiveness in delivering real privacy protection.[154]

Parliament and of the Council on the adequate protection of personal data in Argentina (O.J. L 168, 5th July 2003, p. 19–22).

149 *See* further Ornelas, L. and Rodriguez, K., *Mexico passes Federal DP law*, Privacy Laws & Business International Newsletter, 2010, issue 105, p. 1, 4–5.

150 Most notably the Privacy Act of 1974 and Computer Matching and Privacy Protection Act of 1988. Note also the extensive case law of the Supreme Court on government surveillance measures, pursuant to the Fourth Amendment to the Bill of Rights in the U.S. Constitution, together with the Court's more limited case law dealing directly with data protection (*see* particularly *Whalen v. Roe*, 429 U.S. 589 (1977)). *See* further Schwartz and Reidenberg, *supra* note 12, chapter 4; Solove, D.J., Rotenberg, M. and Schwartz, P.M., *Information Privacy Law*, Aspen Publishers, New York 2006, 2nd rev. edn., chapters 3 and 6; .

151 *See* generally the overview in Schwartz and Reidenberg, *supra* note 12, especially chapters 9–14; Solove, Rotenberg and Schwartz, *supra* note 150, especially chapters 2 and 7.

152 *See* "www.export.gov/safehrbr/list.aspx".

153 Decision 2000/520/EC of 26th July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (O.J. L 215, 25th Aug. 2000, p. 7 *et seq.*).

154 *See* particularly Connolly, C., *How safe is the US Safe Harbor?*, Privacy Laws & Business International Newsletter, 2008, issue 96, p. 1, 3, 26–27 (reporting the results of a study by the consultancy firm, Galexia, which found considerable levels of non-compliance with the scheme). *See* too Dhont, J., Pérez Asinari, M.V., Poullet, Y., Reidenberg, J.R. & Bygrave, L.A., *Safe Harbour Decision Implementation Study*, Report for European Commission (Study Contract PRS/2003/AO-7002/E/27), available via "ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm" (reporting similar findings, though on a more limited empirical base than the Galexia study).

In the Asia-Pacific region, there exist a handful of relatively comprehensive legislative regimes on data protection – most notably those in Australia, New Zealand, Hong Kong, South Korea and Japan.[155] The bulk of these jurisdictions – but not Japan – have also established data protection authorities. New Zealand has been the fastest and most ambitious of these jurisdictions in the data protection field; it was the first to enact data protection legislation applying across the public and private sectors.[156] Australian, South Korean and Japanese legislation in the field was initially limited largely to regulating the data-processing activities of government agencies,[157] but has since been extended to cover the private sector as well.[158] However, some of these extensions still leave large gaps in private sector coverage.[159] Other aspects of the laws in question also diverge from the E.U. model(s).[160] None of the countries concerned has yet been formally recognised by the European Commission as offering adequate protection pursuant to the E.U. Directive.

155 Further on Australian law, *see, e.g.*, Hughes and Jackson, *supra* note 14; on New Zealand law, *see* Roth, P., *Privacy Law and Practice*, Butterworths / LexisNexis, Wellington 1994- (looseleaf, regularly updated); on Hong Kong law, *see* Berthold, M. and Wacks, R., *Hong Kong Data protection Law: Territorial Regulation in a Borderless World*, Sweet & Maxwell, Asia 2003, 2nd ed., and McLeish, R. and Greenleaf, G., *Hong Kong*, in Rule, J.B. and Greenleaf, G. (eds.), Global Privacy Protection: The First Generation, Edward Elgar, Cheltenham 2008, p. 230–256; on South Korean law, *see* Park, W.I., *Republic of Korea*, in Rule, J.B. and Greenleaf, G. (eds.), Global Privacy Protection: The First Generation, Edward Elgar, Cheltenham 2008, p. 207–229; on Japanese law, *see* Case, D. and Ogiwara, Y., *Japan's new personal information protection law*, Privacy Law & Policy Reporter 2003, vol. 10, p. 77–79.

156 *See* Privacy Act of 1993.

157 For Australia, *see* federal Privacy Act of 1988. For Japan, *see* Act for Protection of Computer-Processed Personal Information Held by Government Organs of 1988 (repealed and replaced by the Act on the Protection of Personal Information Held by Government Organs of 2003. For South Korea, *see* Act on Protection of Personal Information Maintained by Public Agencies of 1994.

158 For Australia, *see* federal Privacy Amendment (Private Sector) Act of 2000. For Japan, *see* Act on Protection of Personal Information of 2003. For South Korea, *see* Act on Promotion of Information and Communications Network Utilization and Data Protection of 1999. The latter Act covers private sector entities insofar as these process personal data for profit using telecommunication networks; medical records and credit information are protected under other laws. Regarding Japan, there is also a separate law for incorporated administrative agencies: *see* Act on Protection of Personal Information Held by Incorporated Administrative Agencies of 2003. The Japanese legislative regime is augmented by sets of ministerial guidelines. Note too that several of the Australian States have enacted data protection laws covering their respective government agencies and, to a lesser extent, the health sector: *see, e.g.*, Victoria's Information Privacy Act of 2000 and Health Records Act of 2001.

159 For example, with a few exceptions, the Australian legislation does not apply to "small business operators"; i.e., businesses with an annual turnover of AUD$3 million or less (see federal Privacy Act, sections 6C(1), 6D, 6DA & 6E)). Another major gap is that the legislation does not cover the processing of data by employers about their present and past employees (as long as the processing is directly related to the employment relationship) (section 7B(3)).

160 The Japanese legislation, for example, does not formally distinguish between sensitive and non-sensitive data, and makes relatively extensive use of "opt-out" consent mechanisms.

Data protection regimes in other Asia-Pacific jurisdictions tend to be even more patchy in coverage. Malaysia, for instance, has recently introduced data protection legislation to cover parts of the private sector but lacks equivalent legislation for personal information processed by government agencies.[161] Singapore has so far decided to establish a data protection regime based largely on voluntary, self-regulatory schemes that are linked with its national trust mark programme.[162] As for the People's Republic of China, there exists formal constitutional protection for privacy-related interests, augmented by a patchwork of sectoral laws on point.[163] There have been signals over recent years that the country is on the verge of introducing relatively comprehensive data protection legislation,[164] but no such law has yet been enacted. Much the same can be said of India. Although the country has previously been reported to be considering enactment of a data protection law modelled on the E.U. Directive (largely due to fear that its burgeoning outsourcing industry will flounder without such legislation in place),[165] no such law has yet emerged.[166]

Legal regimes for data protection are least developed in Middle Eastern and African countries taken as a whole. As noted above, the African Charter on Human and People's Rights of 1981 omits mentioning a right to privacy in its catalogue of basic human rights. Moreover, the bulk of African countries have yet to enact European-style data protection laws. Nonetheless, some such laws have recently emerged, chiefly in francophone African states, such as Burkina Faso, Tunisia, Morocco and Mauritius.[167] This development partly reflects

161 *See* further Greenleaf, *supra* note 135.

162 *See* further Tan, *supra* note 108, part IV. For early criticism of the schemes, *see* Greenleaf, G., *Singapore takes the softest privacy options*, Privacy Law & Policy Reporter 2002, vol. 8, p. 169–173.

163 *See* further Lü, *supra* note 59, p. 9–10; Xue, H., *Privacy and personal data protection in China: 2009 update*, Privacy Laws & Business International Newsletter, 2009, December, p. 21–22.

164 *See, e.g.*, Greenleaf, G., *China proposes Personal Information Protection Act*, Privacy Laws & Business International Newsletter, 2008, issue 91, p. 1, 3–6 and references cited therein.

165 *See* Pedersen, A., *India plans EU-style data law*, Privacy Laws & Business International Newsletter, 2003, issue 68, p. 1, 3; Dresner, S., *India gives commitment on new privacy initiative*, Privacy Laws & Business International Newsletter, 2004, issue 72, p. 1, 3, 17.

166 This is not say that there have been no significant legislative developments on point. One such development is enactment of the Credit Information Companies (Regulation) Act of 2005 which provides a relatively comprehensive data protection code for the credit-reporting industry, but this is yet to be put effectively in operation. Another development is enactment of the Information Technology Act of 2000, together with amending legislation of 2008. The legislation contains several provisions dealing with security and wrongful disclosure of personal data (*see, e.g.*, sections 43, 43B, 66, 66B, 72A) but, again, they have yet to be put effectively in operation. Moreover, the small privacy gains they represent are dwarfed by the extensive surveillance measures that are authorized by other provisions in the legislation (*see, e.g.*, section 69B) along with other laws. Further on recent surveillance trends in India, *see* Greenleaf, G., *Data surveillance in India: multiple accelerating paths*, Privacy Laws & Business International Newsletter, 2010, issue 105, p. 15–17.

167 For Burkina Faso, see Act 10-2004/AN on Protection of Personal Data, available at "www.cil.bf/legislations/loi_cil_burkina_faso.pdf"; for Tunisia, see Organic Act n°2004-63

efforts by the French data protection authority (Commission de l'Informatique et des Libertés (CNIL)) to cultivate data protection in former French colonies, but it also reflects economic concerns, particularly the desire by some of these countries to safeguard their outsourcing industry (the case with, e.g., Tunisia and Morocco). Of the non-francophone states, the Republic of South Africa has come furthest along the path to establishing a comprehensive legal regime on data protection. Express provision for a right to privacy is made in section 14 of its Bill of Rights set out in Chapter 2 of its Constitution of 1996. Also included (in section 32) is a broad right of access to information held in both the public and private sectors. Freedom of information (F.O.I.) legislation based on the latter right was enacted in 2002,[168] and work is proceeding on a bill for separate data protection legislation.[169]

As for the Middle East, Israel has long had a legislative regime for privacy and data protection in place,[170] and has been recently assessed by the E.U.'s Article 29 Working Party as passing the E.U. adequacy test.[171] And, as noted above, Dubai passed data protection legislation in 2007 – the first (and hitherto only) Arab state to do so. That legislation, however, applies only to the Dubai International Financial Centre, not to data-processing activities in the rest of Dubai.

---

on Protection of Personal Data, available via "http://www.inpdp.nat.tn/version-anglaise/texte.html"; for Morocco, see Law no. 09-08 on the Protection of Individuals in Relation to Processing of Personal Data; for Mauritius, see Data Protection Act of 2004, available via www.gov.mu/portal/site/dataprotection".

168 *See* Promotion of Access to Information Act of 2000. Further on the Act, *see* Currie, I. and Klaaren, J., *The Promotion of Access to Information Act Commentary*, Siber Ink, South Africa 2002. A unique feature of the legislation is that it provides, as a point of departure, for F.O.I. rights not just in relation to information held by government agencies but also information held in the private sector.

169 *See* Currie and Klaaren, *ibid.*, p. 11, 18; Ncube, C., *A Comparative Analysis of Zimbabwean and South African Data Protection Systems*, Journal of Information, Law and Technology, 2004, no. 2, "www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/".

170 *See* particularly Privacy Protection Act of 1981 (as amended) together with section 7 of the Basic Law on Human Dignity and Liberty.

171 *See* Article 29 Working Party, *Opinion 6/2009 on the level of protection of personal data in Israel* (WP 165, 1st Dec. 2009). The Article 29 Working Party (full title: Working Party on the Protection of Individuals with regard to the Processing of Personal Data), established under Article 29 of the Data Protection Directive, is composed largely of representatives from each EU member state's data protection authority. Its chief task is to provide independent advice to the European Commission on a range of issues, including uniformity in the application of national measures adopted pursuant to the Directive, and privacy protection afforded by non-member states (Article 30). For detailed analysis of its role and achievements, see Poullet, Y. and Gutwirth, S., *The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of "Reflexive Governance"?*, in Pérez Asinari, M.V. and Palazzi, P. (eds.), Défis du Droit à la Protection de la Vie Privée / Challenges of Privacy and Data Protection Law, Bruylant, Brussels 2008, p. 569–609.

5.3 Relative Impact of Regulatory Regimes

Comparative evaluation of the impact of the various regulatory regimes canvassed above is both complex and beset by numerous potential pitfalls. The complexity of the task arises partly from the multiple facets of impact measurement: impact needs to be evaluated in terms of *economy* (i.e., the cost of setting up the regime), *efficiency* (i.e., the cost of the regime measured against its practical results), *effectiveness* (i.e., the extent to which the practical results of the regime fulfil its ultimate aims), and *equity* (i.e., the extent to which the regime extends protection equitably across social groups).[172]

Further complicating matters is that each country's data protection regime consists of more than formal legal rules. While the latter, together with formal oversight mechanisms, are important constituents of a data protection regime, they are supplemented by a complex array of other instruments and institutions – information systems, industry codes, standards, etc. – which concurrently influence the practical impact of the legal rules. The functioning of a data protection regime (including, of course, the extent to which "law in books" equates with "law in practice") will also be shaped by a myriad of relatively informal customs and attitudes which prevail in the country concerned – e.g., the extent to which the country's administrative and corporate cultures are imbued with a respect for authority or respect for "fair information" principles.[173] It goes without saying that many of these factors can be easily overlooked or misconstrued. Their existence means, for instance, that it cannot be assumed that a data protection agency with strong formal powers will necessarily have greater success in fulfilling its objectives than an agency with weaker formal powers.[174]

Yet another complicating element is that the regulatory approach of many data protection agencies can obscure their positive achievements. Agencies frequently prefer to resolve conflict in a relatively quiet way involving "back-room" negotiation rather than publicly striking out with threatened use of punitive sanctions.[175] Further, agencies are often equally, if not more, concerned about curbing an *unrealised potential* for privacy-invasive activity as about providing a remedy after such activity occurs. Measuring the impact of anticipatory forms of control can be more difficult than for reactive, *ex post facto* control forms.[176]

---

172 This classification of criteria is based on Bennett and Raab, *supra* note 39, p. 244 *et seq*.

173 *See* generally Flaherty, D.H., *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill / London 1989.

174 Again, *see* Flaherty, *supra* note 173. Note particularly Flaherty's finding that the German Federal Data Protection Commissioner (Bundesdatenschutzbeauftragter) – which had only advisory powers at the time – had a more profound impact on the federal public sector in (West) Germany than Sweden's Data Inspection Board (Datainspektionen) – which can issue legally binding orders – had on the Swedish public sector: *ibid.*, p. 26.

175 *Id*.

176 For further discussion on the difficulties of comparative assessment of data protection regimes, *see* Bennett and Raab, *supra* note 39, chapter 9; Raab, C.D. and Bennett, C.J., *Taking the measure of privacy: can data protection be evaluated?*, International Review of Administrative Sciences 1996, vol. 62 , p. 535–556.

These problems notwithstanding, a large degree of consensus exists amongst experts in the field regarding the relative strengths of certain data protection regimes. Part of this consensus is a view that the U.S. data protection regime is weaker in fundamental respects than the equivalent regimes in many other countries, particularly those in Europe. A central conclusion of the hitherto most extensive comparative study of the data protection regimes of (West) Germany, the United Kingdom, Sweden, Canada and the U.S.A., is that "the United States carries out data protection differently than other countries, and on the whole does it less well".[177] The major reasons for this finding are the lack of a U.S. federal data protection agency, together with the paucity of comprehensive data protection legislation covering the U.S. private sector. While the finding stems from the late 1980s, it is still pertinent and is backed up by more recent analyses.[178] A basic premise of all these analyses is that the gaps in the U.S. regime are not adequately filled by other measures, such as industry self-regulation and recourse to the courts.

By contrast, the German data protection regime is often viewed as one of the most successful.[179] It has a comprehensive, well-established legislative platform with a firm constitutional footing and several progressive features. One such feature is a legal requirement that organisations appoint internal privacy officers.[180] Another such feature is relatively extensive encouragement of "systemic data protection" ("Systemdatenschutz"); i.e., integration of data protection concerns in the design and development of information systems architecture.[181] The legislation is backed up by comparatively effective oversight and enforcement mechanisms. The effectiveness of these mechanisms appears to be the result of a combination of factors, most notably the seriousness with which Germans generally take data protection issues, the relatively conformist, legalistic nature of German administrative and corporate cultures, the strong, persuasive personalities of the persons who have been appointed data protection commissioners, together with the considerable talents of their staff.[182]

177 Flaherty, *supra* note 173, p. 305.

178 *See, e.g.*, Schwartz and Reidenberg, *supra* note 12, especially p. 379–96; Anderson, D.A., *The Failure of American Privacy Law*, in Markesinis, B.S. (ed.), Protecting Privacy, Oxford University Press, Oxford 1999, p. 139–167; Manny, C., *Incomplete Privacy: How Federal Law Misses Problems Connected to the U.S. Consumer Database Industry*, in Pérez Asinari, M.V. and Palazzi, P. (eds.), Défis du Droit à la Protection de la Vie Privée / Challenges of Privacy and Data Protection Law, Bruylant, Brussels 2008, p. 171–187; Smith, R.E., *Employment Privacy in the U.S.: Only Fragile Protections*, in Pérez Asinari, M.V. and Palazzi, P. (eds.), Défis du Droit à la Protection de la Vie Privée / Challenges of Privacy and Data Protection Law, Bruylant, Brussels 2008, p. 299–316; Gellman, R., *The American Approach to Privacy Protection: Less than the Sum of its Parts*, in Pérez Asinari, M.V. and Palazzi, P. (eds.), Défis du Droit à la Protection de la Vie Privée / Challenges of Privacy and Data Protection Law, Bruylant, Brussels 2008, p. 611–634. Gellman (*ibid.*, p. 634) claims that "Flaherty's conclusion is likely to remain valid for the indefinite future".

179 *See, e.g.*, Flaherty, *supra* note 173, especially p. 21–22.

180 *See* Federal Data Protection Act, sections 4f–4g.

181 *See* particularly Federal Data Protection Act, sections 3a, 9. For further discussion, *see* Bygrave, *supra* note 16, p. 346, 371.

182 *See* generally Flaherty, *supra* note 173, Part 1.

Nevertheless, the data protection regime in Germany does have weak points. Somewhat paradoxically, perhaps the most significant of these is the sheer mass of rules on data protection; the regulatory framework is so dense as to be confusing, non-transparent and unwieldy.[183] Hence, despite its relative success, the German regime still falls short of meeting its policy objectives.

It goes without saying that data protection regimes in most other, if not all, jurisdictions display a similar shortfall. European regimes in general are a noteworthy case in point as they tend to be held up as providing strong levels of data protection in the global context. There has been sporadic evidence that many of these regimes do not outperform the U.S. regime in all respects even if they are, on paper at least, far more comprehensive and stringent than their U.S. counterpart.[184] More significantly, there is relatively extensive, solid evidence indicating weak levels of enforcement, compliance and awareness with respect to many of the European national laws in the field. The first such evidence came to light in the context of the European Commission's first study on the implementation of the E.U. Data Protection Directive in 2002–2003.[185] More recent studies have backed up the findings of the first study.[186] Taken together, the studies show that data protection agencies in Europe are generally under-resourced, leading in turn to under-resourcing of enforcement efforts. Compliance by data controllers is often patchy, though they are generally supportive of the aims of data protection law. While data subjects seem to be increasingly aware of their data protection rights and the legislation setting out those rights, very few of them are aware of the existence of a national data protection authority. Moreover, differences between the various national laws persist which run counter to the harmonising objective of the Directive. Particularly problematic from an international perspective, is that E.U. member states' respective implementations of Articles 25–26 in the Directive has been broadly divergent and, in many cases, inconsistent with the Directive. Indeed, a

183 *See* generally Rossnagel, A., Pfitzmann, A., Garstka, H., *Modernisierung des Datenschutzrechts*, report for the German Federal Ministry of the Interior (Bundesministerium des Innern), September 2001, "www.computerundrecht.de/media/gutachten.pdf".

184 For example, a survey in 2000 of privacy policies posted on U.S.- and E.U.-based internet sites that sell goods or services to consumers, found the policies on the E.U. sites to be no better than the policies on U.S. sites; indeed, some of the latter sites displayed the best policies. *See* Consumers International (Scribbins, K.), *Privacy@net: An international comparative study of consumer privacy on the internet* (January 2001), available via "www.consumersinternational.org/".

185 European Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, Brussels, 15th May 2003, "ec.europa.eu/justice_home/fsj/privacy/lawreport/report_en.htm".

186 *See, e.g.*, E.U. Agency for Fundamental Rights, *Data Protection in the European Union: the Role of National Data Protection Authorities*, Publications Office of the EU, Luxembourg 2010; LRDP KANTOR Ltd. and Centre for Public Reform, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: Final Report*, report for European Commission, 20th January 2010, available via "ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm". For supportive Norwegian evidence on point, *see* Ravlum, I-A., *Behandling av personopplysninger i norske virksomheter*, Transportøkonomisk institutt, Oslo 2006.

substantial amount of transborder data flow is not being subjected to regulation at all.

Finally, account should be taken of several strands of legitimate criticism of data protection regimes *generally*. One line of criticism concerns the regimes' underdevelopment of a systemic focus – as manifest, for instance, in the paucity of direct legislative encouragement for privacy-enhancing technologies.[187] Another line of criticism relates to marginalisation of the judiciary; in many countries, the courts have played little, if any, direct role in developing and enforcing data protection norms. This situation not only results in scarcity of authoritative guidance on the proper interpretation of the relevant legislation but contributes to the marginalisation of data protection as a field of law.[188]

The potentially most damaging line of criticism is that data protection regimes so far have tended to operate with largely procedural rules that do not seriously challenge established patterns of information use but seek merely to make such use more efficient, fair, and palatable for the general public. Legislators' motives for enacting data protection laws are increasingly concerned with engendering public acceptance for new information systems, particularly in the area of electronic commerce. Concomitantly, it is argued that the regimes are incapable of substantially curbing the growth of mass surveillance and control.[189] Although this criticism is valid, it should not be overlooked that some regimes – particularly in Europe – have shown an ability to restrict certain data-processing practices and to raise awareness of the importance of privacy safeguards.[190] Nevertheless, the dykes erected in the name of privacy have seldom been high and thick. More ominously, in an ideological climate dominated by the "war on terrorism", the prospects for building new dykes, let alone reinforcing existing ones, are far from promising.

6 Concluding Remarks – Prospects for Regulatory Consensus

This article highlights widespread concern to protect privacy and related interests, particularly in the face of developments in ICT Regulatory responses to this concern in the form of data protection laws have emerged in many countries. While the most far-reaching of these laws are still predominantly European, readiness to establish at least rudimentary regulatory equivalents is increasingly global. Moreover, data protection laws in the various countries

187 *See* especially Bygrave, *supra* note 16, Part IV.

188 *See* especially Bygrave, *Where have all the judges gone? Reflections on judicial involvement in developing data protection law*, in Wahlgren, P. (ed.), IT och juristutbildning. Nordisk årsbok i rättsinformatik 2000, Jure AB, Stockholm 2001, p. 113–125; also published in Privacy Law & Policy Reporter 2000, vol. 7, p. 11–14, 33–36.

189 *See* especially Rule, J., McAdam, D., Stearns, L., Uglow, D., *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, New York 1980; Flaherty, *supra* note 173.

190 *See, e.g.*, Bygrave, *supra* note 16, chapter 18 and examples cited therein; *see* also Flaherty, *supra* note 173, particularly Part 1.

expound broadly similar core principles and share much common ground in terms of enforcement patterns.

Nevertheless, this article also highlights numerous points of difference between the various data protection regimes. It is pertinent, therefore, to conclude with some brief comments about the chances of achieving greater harmonisation of regimes across the globe. To be blunt, extensive harmonisation at the global level is extremely unlikely to occur in the near future.[191] This is partly because of the strength of ingrained ideological/cultural differences around the world. As noted above, such differences arise even between members of the Western, liberal, democratic sphere and will not disappear quickly. Future international policy making in the field will have to engage seriously with nations and cultures outside that sphere; bridging differences there will be even more daunting. Yet another factor is the lack of a sufficiently strong, dynamic and representative international body to do the bridging work. The World Trade Organisation (W.T.O.) is occasionally touted as such a body. Yet its ability to negotiate a broadly acceptable data protection code will be hampered by its commercial bias. Its ability to negotiate such an agreement quickly and efficiently is also in doubt given its track record in other policy areas.[192]

Augmenting these difficulties is increasing clutter on the horizons for regulatory policy generally:

> "Forty years ago the ideological landscape in which international privacy instruments were drafted was more open than now. Back then, discussion about privacy revolved largely about doctrines on human rights and rule of law; economic and trade-related considerations received relatively marginal attention. Today, however, the same sort of discussion cannot be separated from trade issues. Nor can it be separated from attention to a range of other cross-cutting issues, such as the "war on terror", national security and law enforcement generally. Globalisation processes in terms of economy, crime, law enforcement, information and communication networks, etc. are rapidly decreasing the size of the world. The horizons for regulatory policy are increasingly cluttered; various norm sets are more prone to colliding with each other. Concomitantly, future international policy making on privacy issues will be increasingly complicated and, arguably, increasingly destined to fail in terms of offering clear and relatively stringent norms".[193]

As for harmonisation efforts at the regional level, the track record of A.P.E.C. is yet to be firmly established. Within the E.U. – home to the hitherto most ambitious efforts – harmonisation remains incomplete. A large question mark hangs also over the ability of the E.U. to bring the data protection regimes of

191 *See* too, e.g., Reidenberg, J.R., *Resolving Conflicting International Data Privacy Rules in Cyberspace*, Stanford Law Review, 2000, vol. 52, p. 1315–1371 (analysing the problems of achieving international harmonization on data protection issues).

192 Witness, for instance, its tardiness in crystallising policy on electronic commerce. See further Wunsch-Vincent, S., *WTO, E-Commerce, and Information Technologies: From the Uruguay Round through the Doha Development Agenda*, Report for U.N. I.C.T. Task Force (Markle Foundation 2005), "www.iie.com/publications/papers/wunsch1104.pdf".

193 Bygrave, *supra* note 79, p. 48.

non-European states in line with its preferred model. This is presently due not so much to the recent emergence of A.P.E.C. as a potential competitor in the role of data protection "superpower"; there is as yet little evidence to show that A.P.E.C. can offer close competition in this regard. Rather, the weak implementation of Articles 25–26 in the E.U. Directive is more immediately critical. How those rules are implemented, constitutes an important litmus test for the Directive's international credibility and success. Significant problems with E.U. member states' implementation of those rules are noted above. The European Commission's tardiness in issuing adequacy findings exacerbates these problems. In the space of over a decade, only a handful of countries have so far received an adequacy stamp – and most of them are scarcely major powers in a global context.[194] This tardiness is not surprising: proper adequacy assessments are inevitably intricate, time-consuming tasks. Unfortunately for the Directive, its regime for transborder data flow to third countries is caught between "a rock and a hard place": if *properly* implemented, the regime is likely to collapse from the weight of its cumbersome, bureaucratic procedures. Alternatively, it could well collapse because of large-scale avoidance of its proper implementation due precisely to fears of such procedures.

194 They include the Faroe Islands, the Bailiwick of Guernsey, the Bailiwick of Jersey, the Isle of Man, Switzerland, Argentina and will soon be joined by Israel and Andorra. For a full list, see "ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm".