Privacy Protection in a Global Context – A Comparative Overview

Lee A. Bygrave

[Published in *Scandinavian Studies in Law*, 2004, vol. 47, p. 319–348]

1 Introduction

Over the last four decades there has been an enormous growth in the field of law and policy which directly addresses privacy-related concerns, particularly with respect to the processing of personal information. While certainly not old, the field has now attained considerable maturity, spread and normative importance. It is augmented by an immense body of commentary analysing privacy issues from a variety of perspectives.

Surprisingly, up-to-date comparative overviews of this development are scarce. This article is an attempt to lessen some of the gaps.

The article outlines the principal similarities and differences between the main national and regional regulatory measures taken to protect privacy in the context of information processing. Comparison is made not only of regulatory strategies but also various national/regional/cultural conceptualisations of the ideals and rationale of privacy protection. Concomitantly, an attempt is made to draw out and synthesise the main findings of the academic literature on the subject.

While much of the article has a legal orientation, its approach is essentially cross-disciplinary. For the most part, the analysis is broad-brush; the focus of the article is the "big picture".

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 (I.C.T.). 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.[1] 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.[2] 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".[3]

The U.S. debate, particularly in the 1960s and early 1970s, about the privacy-related threats posed by modern I.C.T. exercised considerable influence on debates in other countries. As Hondius writes, "[a]lmost every issue that arose in

---

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

2 *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.

3 The title of Westin's seminal work, *Privacy and Freedom*, *supra* note 2, 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.

Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale".[4] 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[5] and in international forums where English is a working language.[6] Yet also in countries in which English is not the main 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),[7] "die Privatsphäre" (German),[8] "privatlivets fred" (Danish/Norwegian).[9]

Nevertheless, the field of law and policy which crystallised from the early discussions in Europe on the privacy-related threats posed by I.C.T. has increasingly 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".[10] 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[11] – it has gained

---

4 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.

5 *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.

6 As is evident, e.g., in the titles of the early Council of Europe resolutions dealing with I.C.T. 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).

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

8 *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.

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

10 Further on the origins of "Datenschutz", *see* Simitis, S. (ed.), *Kommentar zum Bundesdaten-schutzgesetz*, Nomos Verlagsgesellschaft, Baden-Baden 2002, 5th ed., p. 3–4.

11 Moreover, it tends to misleadingly connote, at least in U.S. circles, concern for security of

broad popularity in Europe[12] and, to a lesser extent, elsewhere.[13] Its use, though, is being increasingly supplemented by the term "data privacy".[14] Arguably, the latter nomenclature is more appropriate as it better communicates the central interest(s) at stake and provides a bridge for synthesising North American and European policy discussions.

At the same time, 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.[15] Norwegian discourse revolves around the concept of "personvern" ("protection of person(ality)"),[16] while Swedish discourse focuses on "integritetsskydd" ("protection of (personal) integrity").[17] 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.[18]

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, long-winded – debate has raged, predominantly in U.S. circles, about which definition is most correct.[19] We find parallel debates in

---

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.

12 *See, e.g.*, Hondius, *supra* note 4.

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

14 *See, e.g.*, Schwartz and Reidenberg, *supra* note 11; Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, Oxford 2003.

15 *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 in 2001) § 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")).

16 *See* Bygrave, L.A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague / London / New York 2002, p. 138–143 and references cited therein.

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

18 *See* Guadamuz, A., *Habeas Data: The Latin American Response to Data Protection*, The Journal of Information, Law and Technology 2000, no. 2, <http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html>; 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*.

19 For useful overviews, *see* 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.

other countries which centre on similar concepts,[20] 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 defining privacy.[21] One set of definitions is in terms of *non-interference*,[22] another in terms of *limited accessibility*.[23] A third set of definitions conceives of privacy as *information control*.[24] 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.[25]

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 privacy.[26] 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),[27] 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).[28] The notion and the right to which it attaches, have had considerable impact on development of data privacy law and policy in Germany[29] and, to a lesser extent, other European countries.

---

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

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

22 *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").

23 *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").

24 *See, e.g.*, Westin, *supra* note 2, 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").

25 *See, e.g.*, Inness, *supra* note 19, 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").

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

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

28 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*.

29 *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

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. Concomitantly, property rights doctrines have rarely been championed as providing a desirable basis for data privacy rules.[30] The relatively few proponents of a property rights approach have tended to come from the U.S.A.,[31] though sporadic advocacy of such an approach also occurs elsewhere.[32]

3 Conceptualisations of the Values Served by Privacy

How do various nations (and/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*.[33] They are, in the words of Westin, largely about "achieving individual goals of self-realization".[34] 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".[35] This view carries sometimes over into claims that privacy rights can be detrimental to societal needs.[36]

---

principles inherent in the right).

30 Opposition to a property rights approach is expressed in, *e.g.*, Miller, *supra* note 2, p. 211; Hondius, *supra* note 4, 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.

31 *See, e.g.*, Westin, *supra* note 2, 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 1996, p. 159–162; Rule, J 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.

32 *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.

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

34 Westin, *supra* note 2, p. 39.

35 *See* Regan, *supra* note 1, chapters 2, 8 and references cited therein.

36 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.[37] 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 privacy policy in the bulk of advanced industrial states.[38]

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 privacy 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.[39] This perspective is under-developed in U.S. jurisprudence.[40]

We find also increasing recognition in *academic* discourse on both sides of the Atlantic that data privacy norms are valuable not simply for individual persons but for the maintenance of societal civility, pluralism and democracy.[41]

A related development is increasing academic recognition that data privacy laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualisations of privacy.[42] This insight is perhaps furthest developed in Norwegian discourse, which has elaborated relatively sophisticated models of the various interests promoted by data privacy laws.[43] These interests include ensuring adequate quality of personal information, "citizen-friendly" administration, proportionality of control, and rule of law. In Norway, the insight that data privacy laws are concerned with more than safeguarding privacy, extends beyond the academic community and into regulatory bodies. Indeed, Norway's principal legislation on data privacy contains an objects clause

---

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

37 *See* Bennett, C.J. and Raab, C.D., *The Governance of Privacy. Policy instruments in global perspective*, Ashgate, Aldershot 2003, chapt. 1.

38 *Ibid.*

39 *See* especially the decision of 15th December 1983, *supra* note 28.

40 *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.

41 *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 1; Ruiz, *supra* note 40; 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 37.

42 *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.

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

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.[44]

The equivalent laws of some other European countries also contain objects clauses embracing more than privacy. The broadest – indeed, boldest – expression of aims is found in the French legislation: "Data processing shall be at the service of every citizen. It shall develop in the context of international co-operation. It shall infringe neither human identity, nor the rights of man, nor privacy, nor individual or public liberties".[45]

Also noteworthy is the express concern in the data privacy 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.[46]

However, considerable uncertainty still seems to reign in many countries about exactly which interests and values are promoted by data privacy laws. This is reflected partly in academic discourse,[47] partly in the absence in some laws of objects clauses formally specifying particular interests or values which the legislation is intended to serve,[48] and partly in the vague way in which existing objects clauses are often formulated.[49]

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

---

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

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

46 *See* further Bygrave, *supra* note 16, p. 39; Simitis, *supra* note 10, p. 11.

47 *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 E.C. Commission, October 1998, "http://europa.eu.int/comm/internal_market/privacy/studies/legal_en.htm" (last accessed 10th June 2004), 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").

48 *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*).

49 *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 goals as protection of "rights and fundamental freedoms, and in particular … right to privacy").

protection.[50] Such difficulty is partly due to paucity of systematically collected empirical data,[51] 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[52] have generally been treated with a great deal of antipathy, yet video surveillance of public places in the U.K.[53] seems to be considerably more extensive than in Scandinavian countries.

It is clear that 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.[54] 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.[55]

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".[56]

---

50 Equally problematic, of course, is the accurate comparison of privacy levels across historical periods. 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 37, chapt. 2.

51 As Bennett and Raab (*supra* note 37, p. 15) 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".

52 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.

53 Further on this surveillance, *see, e.g.*, *Der Spiegel*, 5th July 1999, p. 122–124; Webb, A., *Spy cameras vs. villains in Britain*, United Press International, 8th March 2002, "http://www.upi.com/view.cfm?StoryID=08032002-020813-4448r" (last accessed 6th July 2004).

54 *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.

55 *See, e.g.*, Moore's study (*supra* note 54) of the Siriono Indians in Bolivia; and Flaherty's study of colonial society in New England (Flaherty, D.H., *Privacy in Colonial New England*, University Press of Virginia, Charlottesville 1972).

56 Moore, *supra* note 54, p. 276. *Cf., inter alia*, Lunheim, R. and Sindre, G., *Privacy and*

However, technological-organizational factors are not the sole determinants of privacy levels. Also determinative are ideological factors. Central amongst these are attitudes to the value of private life,[57] attitudes to the worth of persons as individuals,[58] and sensitivity to human beings' non-economic and emotional needs.[59] 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".[60]

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 rights is increasingly on the legislative agenda of some African countries. A similar development is occurring in some Asian jurisdictions.

Moreover, it should be kept in mind that, in the U.S.A. – often portrayed as the citadel of liberal ideals – legal protection of privacy falls short in significant respects of the protection levels in 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 privacy legislation regulating the U.S. private sector and of an independent agency ("data protection authority" or "privacy commissioner") to specifically oversee regulation of data privacy matters.[61] Thus, within the Western liberal democratic "camp", considerable variation

---

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.

57 *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 54, 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.

58 *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).

59 *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).

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

61 *See* also section 5.2. Further on the differences between U.S. and European regulatory approaches in the data privacy field, *see, e.g.*, Charlesworth, A., *Clash of the Data Titans? US and EU Data Privacy Regulation*, European Public Law 2000, vol. 6, p. 253–274; Reidenberg, J.R., *Resolving Conflicting International Data Privacy Rules in Cyberspace*, Stanford Law Review 2000, vol. 52, p. 1315, 1330 *et seq*.

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).[62] 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 privacy regulation in Europe[63] 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.

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 many other countries to curb domestic civil liberties, including privacy rights.[64]

Yet other factors can play a role too. For instance, U.S. and, to a lesser extent, Australian eschewal of "omnibus" data privacy 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.[65]

---

62 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 47, 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.

63 *See* section 5.2.

64 *See* generally Electronic Privacy Information Center (EPIC) and Privacy International (PI), *Privacy and Human Rights 2003. An International Survey of Privacy Laws and Developments*, EPIC / PI, Washington, D.C. 2003.

65 With respect to U.S. attitudes, *see, e.g.*, Schwartz and Reidenberg, *supra* note 11, p. 6 *et seq.* For further analysis of the causes of divergence between Western countries' respective regimes for data privacy, *see* Bennett, C.J., *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca 1992, chapt. 6.

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.[66] There is abundant evidence from public opinion surveys that these levels of concern and support are relatively high,[67] at least in the abstract.[68] The concern for privacy is often accompanied by considerable pessimism over existing levels of privacy, along with lack of trust that organisations will not misuse personal information.[69] Privacy concern tends to cut across a broad range of political leanings (within liberal democratic ideology),[70] though there are occasional indications of statistically significant variation in attitudes to privacy issues based on party-political attachments.[71] 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.[72]

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.[73] 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

---

66 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.

67 *See, e.g.*, Bygrave, *supra* note 16, p. 110 and references cited therein; Bennett and Raab, *supra* note 37, 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. 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.

68 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.

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

70 *See* further Bennett, *supra* note 55, especially p. 147.

71 *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 privacy as important than were supporters of the more conservative political parties).

72 *Compare, e.g.*, Székely, *supra* note 67 (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).

73 *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).

divulge personal information and a concomitant adjustment of what they perceive as problematic for their privacy. Unfortunately, there seems to be little survey evidence addressing this point.

Nevertheless, public concern for privacy has rarely resulted in mass political movements with privacy protection *per se* high on their agenda.[74] In most Western countries and, even more so, on the international plane, actual formulation of law and policy on data privacy has typically been the project of a small elite.[75] 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'".[76] This would be, however, an inaccurate (and unfair) characterisation of the modern "data privacy 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.[77]

5 Regulatory Policy on Protection of Privacy and Personal Information (Data Privacy)

This section provides an overview of the main legal instruments at both international and national levels which deal directly with data privacy.[78] Some 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.

---

74 *See* generally Bennett, *supra* note 65, p. 146, 243.

75 *Ibid.*, p. 127 *et seq.*

76 Westin, *supra* note 2, 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.

77 *See* also Bennett, *supra* note 65, p. 129.

78 At the risk of stating the obvious: to describe these instruments as dealing directly with "data privacy" is to indicate that they specifically regulate all or most stages in the processing of personal data – i.e., data that relate to, and facilitate identification of, an individual, physical/natural person (or, sometimes, collective entity) – with a principal formal aim of safeguarding the privacy and/or related interests of that person. The main rules applied to the processing of such data embody a set of largely procedural, "fair information" principles stipulating, e.g., the manner and purposes of data processing, measures to ensure adequate quality of the data, and measures to ensure transparency of the processing in relation to the person to whom the data relate ("data subject"). For more detail, *see* generally Bygrave, *supra* note 16, particularly chapters 1, 3, 5, 18, 19.

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 privacy 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 privacy. Also of primary interest is the degree to which countries provide for the establishment of independent agencies (hereinafter termed "data privacy agencies") specifically charged with overseeing the implementation and/or further development of these rule-sets.

5.1 International Instruments

The formal normative basis for data privacy 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.),[79] the International Covenant on Civil and Political Rights (I.C.C.P.R.)[80] along with the main regional human rights treaties, such as the European Convention on Human Rights and Fundamental Freedoms (E.C.H.R.)[81] and the American Convention on Human Rights (A.C.H.R.).[82] All of these instruments – with the exception of the African Charter on Human and People's Rights[83] – expressly recognise privacy as a fundamental human right.[84] 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[85] 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 privacy 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 privacy laws frequently single out protection of that right as central to their formal rationale.[86] It is also reflected in case law developed pursuant to

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

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

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

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

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

84 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).

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

86 *See, e.g.*, Article 1 of the Council of Europe Convention on data privacy, *supra* note 49; 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*

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 privacy laws.[87] Indeed, these provisions function, in effect, as data privacy instruments in themselves. However, case law has yet to apply them in ways that add significantly to the principles already found in other data privacy 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.[88]

In terms of other international legal instruments, there does not exist a truly global convention or treaty dealing specifically with data privacy. Calls for such an instrument are occasionally made, though there are no concrete plans afoot to draft one. The closest to such an instrument is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "C.o.E. Convention").[89] While 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 (see Article 23). However, it has yet to be ratified by a non-member state.

Within the E.U., several Directives on data privacy have been adopted, the first and most important of which 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").[90] This instrument is

---

à caractère personnel); preamble to (and title of) Australia's federal Privacy Act of 1988.

87 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) Reports of Judgments and Decisions of the European Court of Human Rights 2000-I; *Von Hannover v. Germany*, Application no. 59320/00, decision of 24th June 2004. *See* further 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.

88 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 it usually is under ordinary data privacy laws: *see* Bygrave, *supra* note 87, p. 277 *et seq*. However, uncertainty surrounding the degree to which Article 8 may be applied in cases involving data-processing practices of the private sector has been significantly reduced with the recent judgment by the European Court of Human Rights in *Von Hannover v Germany*, Application no. 59320/00, decision of 24th June 2004 (confirming such application).

89 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 16, especially p. 32.

90 Adopted 24th Oct. 1995 (Official Journal of the European Communities (O.J.), L 281, 23rd Nov. 1995, p. 31 *et seq.*). Two sectoral Directives on data privacy have also been adopted. The first of these was Directive 97/66/EC of 15th Dec. 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (O.J. L 24, 30th Jan. 1998, p. 1 *et seq.*). This has now been replaced by Directive 2002/58/EC of 12th July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (O.J. L 201, 31st July 2002, p. 37 *et seq.*). Further on the general Directive, *see, e.g.*, Bainbridge, D.I., *EC Data Protection Directive*, Butterworths,

binding on E.U. member states. It is also binding on non-member states (Norway, Iceland and Liechtenstein) that are party to the 1992 Agreement on the European Economic Area (E.E.A.). While the Directive is primarily a European instrument for European states, it exercises considerable influence over other countries not least because it prohibits (with some qualifications) transfer of personal data to those countries unless they provide "adequate" levels of data privacy (see Articles 25–26).[91] As shown below, many non-European countries are passing legislation in order, at least partly, to meet this adequacy criterion.[92] Furthermore, the Directive stipulates that the data privacy law of an E.U. state may apply outside the E.U. in certain circumstances, most notably if a data controller,[93] 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)).[94] All of these provisions give an impression that the E.U., in effect, is legislating for the world.[95]

Apart from the above legal instruments, there exist numerous international and regional instruments on data privacy 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 privacy 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.).[96] The Guidelines contain a set of data privacy

---

London / Dublin / Edinburgh 1996; Damman, U. and Simitis, S., *EG-Datenschutzrichtlinie: Kommentar*, Nomos Verlagsgesellschaft, Baden-Baden 1997.

91 *See, e.g.*, Kuner, *supra* note 14, chapter 4.

92 Further on this influence, *see* 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.

93 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).

94 *See* further Bygrave, L.A., *Determining Applicable Law pursuant to European Data Protection Legislation*, Computer Law & Security Report 2000, vol. 16, p. 252–257; Kuner, *supra* note 14, chapter 3.

95 Equally, they nourish accusations of "regulatory overreaching". *See* particularly the criticism of Article 4(1)(c) in Bygrave, *supra* note 94. *See* also the more general criticism (from U.S. and Australian quarters) in 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.

96 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. The O.E.C.D. has issued other guidelines also relating, albeit more indirectly, to data privacy: 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 July 25th 2002); Guidelines for Cryptography Policy (adopted 27th March

principles similar to those stipulated in the C.o.E. Convention. The Guidelines have been very influential on the drafting of data privacy laws and standards in non-European jurisdictions, such as Australia, New Zealand and Canada.[97] They have also been formally endorsed – though not necessarily implemented – by numerous companies and trade associations in the U.S.A.[98] Further, they constitute an important point of departure for ongoing efforts by the Asia Pacific Economic Cooperation (A.P.E.C.) to draft a set of common data privacy principles for jurisdictions in the Asia Pacific region.[99]

Of potentially broader reach are the United Nations (U.N.) Guidelines Concerning Computerized Personal Data Files (hereinafter "U.N. Guidelines"), adopted 1990.[100] The Guidelines are intended to encourage enactment of data privacy 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.[101] Nevertheless, their adoption underlines that data privacy 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.[102]

Note should also be taken of the numerous recommendations, codes, etc. which are of sectoral application only. The C.o.E., for instance, has issued a large range of sector-specific recommendations to supplement and extend the rules in its Convention on data privacy. These recommendations cover, *inter alia*, the police sector,[103] employment,[104] research and statistics,[105] and

---

1997); and Guidelines for Consumer Protection in the Context of Electronic Commerce (adopted 9th Dec. 1999).

97 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 95. 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.

98 *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.

99 See generally the documentation collated at "http://www.apecsec.org.sg/apec/documents_reports/electronic_commerce_steering_group/2004.html" (last accessed 8th July 2004).

100 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.

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

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

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

telecommunications.[106] Another noteworthy instance is the code of practice issued by the International Labour Organization (I.L.O.) on data privacy in the workplace.[107]

The principal international instruments dealing specifically with data privacy 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 privacy as facilitating the flow of personal data across national borders in order to maintain international commerce, freedom of expression, and inter-government cooperation.[108] The latter concerns arise because many national data privacy laws – mainly European – have long operated with rules providing for restrictions of data flow to countries not offering levels of data privacy similar to the "exporting" jurisdiction.[109] While the practical effect of such rules on actual transborder data flow tends to have been, for the most part, negligible,[110] 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 and E.U. Directive.[111] The latter goes the furthest in securing 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.[112] At the same time, however, the Directive goes the 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 privacy (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 privacy regimes,[113] but

---

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

105 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).

106 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).

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

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

109 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.

110 *See, e.g.*, the extensive survey in Ellger, *supra* note 109.

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

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

113 *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.

little solid evidence exists to support them.[114] While there is perhaps more evidence linking the origins of the Directive to protectionist concerns, the linkage is still tenuous.[115] 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,[116] in recent case law from the European Court of Justice,[117] and, increasingly, in the E.U. legal system generally. Particularly noteworthy is growing recognition in the E.U. that protection of data privacy is in itself (i.e., separate from the broader right to privacy) a basic human right.[118]

Despite their harmonising objectives, the international instruments tend to leave countries a significant degree of leeway in development of their respective data privacy 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.[119] 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.[120]

Of all of the instruments canvassed above, the E.U. Directive has become the leading trendsetter and benchmark for data privacy 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 recently 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 privacy authorities.[121] Outside Europe, clear traces of the Directive are to be found in the draft Guidelines on the Protection of Personal Information and Privacy drawn up by the Asia Pacific

---

1055–1103; Pinegar, K.R., *Privacy Protection Acts: Privacy Protectionism or Economic Protectionism?*, International Business Lawyer 1984, vol. 12, p. 183–188.

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

115 *Id.*

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

117 *See* especially judgment of 20th May 2003 in Joined Cases C-465/00, C-138/01, and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-0000, particularly paragraph 71 *et seq*.

118 *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). See also the right to protection of personal data in Article I-50 of the draft Treaty establishing a Constitution for Europe (CIG 86/04, Brussels, 18th June 2004).

119 *See* Henke, *supra* note 89, especially p. 57–60; Bygrave, *supra* note 16, p. 34.

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

121 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (C.E.T.S. No. 181; adopted 23rd May 2001; in force 1st July 2004).

Telecommunity,[122] and in the draft Asia-Pacific Privacy Charter drawn up by the Asia-Pacific Privacy Charter Council (A.P.P.C.C.).[123]

Nevertheless, the leadership status of the Directive could face serious challenge in the Asia Pacific region if A.P.E.C. is able to agree on a common set of data privacy principles for its 21 member states. There are indications that the principles are likely to be inspired more by the O.E.C.D. Guidelines than the Directive, at the same time as they are likely to be less privacy-protective than the Directive and possibly the Guidelines.[124] Work on the principles signals a readiness amongst many of the A.P.E.C. states to forge their own approach to data privacy without necessarily conforming to European norms. This approach would appear to foster data privacy regimes less because of concern to protect basic human rights than concern to engender consumer confidence in business.[125]

5.2 National Instruments

Well over thirty countries have enacted data privacy laws, and their number is growing steadily.[126] The bulk of these countries are European. Indeed, Europe is home to the oldest, most comprehensive and most bureaucratically cumbersome data privacy laws at both national and provincial levels. Moreover, as shown 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 privacy 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";

---

122 Draft of Sept. 2003; on file with author but not publicly available.

123 *See* Version 1.0 of the Charter, dated 3rd Sept. 2003; on file with author but not publicly available. Further on the A.P.P.C.C. and its work, *see* "http://www.bakercyberlawcentre.org/appcc/" (accessed 25th July 2004).

124 *See, e.g.*, Greenleaf, G., *APEC's privacy standard regaining strength*, Privacy Law & Policy Reporter 2004, vol. 10, p. 158–157.

125 *See* Tang, *Personal Data Privacy: The Asian Agenda*, speech given at 25th International Conference of Data Protection and Privacy Commissioners, Sydney, 10th Sept. 2003, available via "http://www.privacyconference2003.org/program.asp#psa" (last accessed 10th July 2004).

126 *See* generally Electronic Privacy Information Centre / Privacy International, *supra* note 64, which gives a fairly up-to-date overview of the state of data privacy regimes in over 50 countries. A complementary, though less comprehensive, overview is given in Henry, M. (ed.), *International Privacy, Publicity and Personality Laws*, Butterworths, London 2001.

- application of extensive sets of procedural principles some of which are rarely found in data privacy regimes elsewhere;[127]
- 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 privacy agencies with broad discretionary powers to oversee implementation and development of data privacy 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 privacy agencies;
- extensive use of "opt-in" requirements for valid consent by data subjects;
- little use of industry-developed codes of practice.[128]

The bulk of these characteristics were originally typical for data privacy laws in West European countries. Due largely to the E.U. Directive, they are now also typical for the laws of most East European countries after their accession to the Union on 1st May 2004. Nevertheless, it is important to note that each country has its own unique mix of rules;[129] concomitantly, a good deal of variation exists in the degree to which each country shares the above-listed traits.[130] For example, the Netherlands has always made relatively extensive use of industry-

---

127 An example of a principle that is unique to 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.

128 For further details, *see, e.g.*, Bygrave, *supra* note 16, chapts. 2–4; Kuner, *supra* note 14.

129 *See, e.g.*, with respect to German law, Simitis, *supra* note 10. With respect to Swedish law, *see, e.g.*, Öman, S. and Lindblom, H.-O., *Personuppgiftslagen: En kommentar*, Norstedts Juridik, Stockholm 2000. With respect to Italian law, *see, e.g.*, Buttarelli, G., *Banche dati e tutela della riservatezza: La privacy nella Società dell'Informazione*, Giuffrè Editore, Milan 1997. With respect to Swiss law, *see, e.g.*, Maurer, U. and Vogt, N.P. (eds.), *Kommentar zum Schweizerischen Datenschutzgesetz*, Helbing & Lichtenhahn, Basel / Frankfurt am Main 1995. With respect to Danish law, *see, e.g.*, Nielsen, K.K. and Waaben, H., *Lov om behandling af personoplysninger – med kommentarer*, Jurist- og Økonomforbundets Forlag, Copenhagen 2001. With respect to Norwegian law, *see, e.g.*, Schartum, D.W. and Bygrave, L.A., *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*, Fagbokforlaget, Bergen 2004.

130 *See* generally Korff, D., *EC Study on Implementation of Data Protection Directive – Comparative summary of national laws*, report commissioned by E.C. Commission, September 2002, "http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf" (last accessed 28th July 2004).

based codes of practice, and the E.U. Directive itself encourages greater use of such codes (see Article 27). Moreover, data privacy 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 and cut back notification requirements to a minimum.[131] There is movement too at a broader European level. For instance, while West European data privacy regimes have traditionally relied heavily on paternalistic control mechanisms,[132] they now show greater readiness to rely more on participatory control,[133] 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 comes closest of the North American countries to embracing the European approach. There is now federal legislation in place to ensure comprehensive protection of data privacy in relation to both the public and private sectors.[134] Some provinces have already enacted data privacy legislation in relation to provincial and local government agencies and/or the private sector.[135] Data privacy agencies exist at both federal and provincial levels. The Commission of the European Communities (hereinafter "European Commission") has formally ruled that, in general, Canada offers "adequate" protection for data privacy pursuant to Article 25 of the E.U. Directive.[136]

By contrast, the U.S. legal regime for data privacy is much more atomised. While there is fairly comprehensive legislation dealing with federal government agencies,[137] omnibus legislative solutions are eschewed with respect to the private sector. Legal protection of data privacy 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.[138] European-style data privacy agencies do not exist. 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

---

131 *See* Personal Data Act of 1998 (*Personuppgiftslagen*, S.F.S 1998:204), sections 36–37.

132 That is, control exercised by government bodies (primarily data privacy agencies) on behalf and supposedly in the best interests of citizens (data subjects).

133 That is, control exercised by citizens themselves.

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

135 *See, e.g.,* Quebec's Act on Protection of Personal Information in the Private Sector of 1993.

136 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.*).

137 Most notably the Privacy Act of 1974 and Computer Matching and Privacy Protection Act of 1988. Note also the limited protection of data privacy afforded under the Constitution as construed by the Supreme Court: *see* especially *Whalen v. Roe*, 429 U.S. 589 (1977). *See* further Schwartz and Reidenberg, *supra* note 11, chapter 4.

138 *See* generally the overview in Schwartz and Reidenberg, *supra* note 11, especially chapters 9–14.

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. The scheme, which so far has attracted over 500 companies,[139] has been held by the European Commission to satisfy the Directive's adequacy test in Article 25.[140]

In South America, Argentina has come furthest in developing a comprehensive legal regime for data privacy. It enacted legislation in 2000[141] 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).[142] The European Commission has formally ruled that Argentina satisfies the adequacy criterion of the E.U. Directive.[143] Other South American countries, such as Brazil and Chile, also provide Constitutional protections for rights privacy and *habeas data*, but otherwise their legislation on data privacy is relatively scant. They lack also data privacy agencies.[144]

In the Asia-Pacific region, there exist a handful of relatively comprehensive legislative regimes on data privacy – most notably those in Australia, New Zealand, Hong Kong, Korea and Japan.[145] The bulk of these jurisdictions – but not Japan – have also established data privacy agencies. New Zealand has been the fastest and perhaps most ambitious of these jurisdictions in the data privacy field; it was the first to enact data privacy legislation applying right across the public and private sectors.[146] Australian, Korean and Japanese legislation in the field was initially limited largely to regulating the data-processing activities of

---

139 *See* "http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list" (accessed 6th July 2004).

140 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.*). However, the scheme is presently under review by the Commission.

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

142 *See* further Electronic Privacy Information Center and Privacy International, *supra* note 64, p. 132–139.

143 Decision C(2003) 1731 of 30th June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (O.J. L 168, 5th July 2003, p. _ *et seq.*).

144 *See* further Electronic Privacy Information Center and Privacy International, *supra* note 64, p. 167–171, 195–197.

145 Further on Australian law, *see, e.g.*, Hughes and Jackson, *supra* note 13; on New Zealand law, *see* Longworth, E. and McBride, T., *The Privacy Act: A Guide*, GP Publications, Wellington 1994 and 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 Privacy Law: Territorial Regulation in a Borderless World*, Sweet & Maxwell, Asia 2003, 2nd ed.; on Korean law, *see* Yi, C.-B. and Ok, K.-J., *Korea's personal information protection laws*, Privacy Law & Policy Reporter 2003, vol. 9, p. 172–179 and Chung, H.-B., *Anti-spam regulations in Korea*, Privacy Law & Policy Reporter 2003, vol. 10, p. 15–19; 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.

146 *See* Privacy Act of 1993.

government agencies,[147] but has recently been extended to cover the private sector as well.[148] However, some of these extensions still leave large gaps in private sector coverage.[149] Other aspects of the laws in question also diverge from the E.U. model(s).[150] Not surprisingly, none of the countries concerned has yet been formally recognised by the European Commission as offering adequate protection pursuant to the E.U. Directive.

Data privacy regimes in other Asia-Pacific jurisdictions tend to be rather patchy in coverage and enforcement levels. Thailand, for instance, has inserted data privacy rules covering the government sector, in legislation dealing primarily with freedom of government information.[151] Singapore has so far decided to establish a data privacy regime based on voluntary, self-regulatory schemes that are linked with its national trust mark programme.[152] The primary catalyst for the schemes appears to be commercial concerns.[153] As for the People's Republic of China, it lacks any credible data privacy regime. While some legal rules have been adopted which potentially provide indirect protection for data privacy,[154] their operational potential is rendered nugatory by a political culture that traditionally shows scant respect for personal privacy.[155] Moreover, there is little, if any, sign that China is ready to adopt more effective data privacy rules in order to meet E.U. adequacy standards. By contrast, India is reported to be considering enactment of a data privacy law modelled on the E.U. Directive

147 For Australia, *see* Privacy Act of 1988; for Japan, *see* Act for Protection of Computer-Processed Personal Data Held by Administrative Organs of 1988; for Korea, *see* Act on Protection of Personal Information Maintained by Public Agencies of 1994.

148 For Australia, *see* Privacy Amendment (Private Sector) Act of 2000; for Japan, *see* Privacy Law of 2003; for Korea, *see* Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. of 1999. Note too that several of the Australian States have enacted data privacy 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.

149 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)).

150 The Japanese laws, for example, do not formally operate with a distinction between sensitive and non-sensitive data, and they make relatively extensive use of "opt-out" consent mechanisms.

151 *See* Official Information Act of 1997, described in Opassiriwit, C., *Thailand: a case study in the interrelationship between freedom of information and privacy*, Privacy Law & Policy Reporter 2002, vol. 9, p. 91–95.

152 *See* Model Data Protection Code for the Private Sector of 2002; Industry Content Code of 2002.

153 For criticism of the schemes, *see* Greenleaf, G., *Singapore takes the softest privacy options*, Privacy Law & Policy Reporter 2002, vol. 8, p. 169–173.

154 *See* further Electronic Privacy Information Center and Privacy International, *supra* note 64, p. 197–200.

155 *Ibid.*, p. 200–210.

largely due to a fear that its burgeoning outsourcing industry will flounder without such legislation in place.[156]

Legal regimes for data privacy are least developed in the 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, none of the African countries have enacted comprehensive data privacy laws.

Nevertheless, some countries display increasing interest in legislating on data privacy. This is partly due to the obligations imposed by the I.C.C.P.R. Article 17. It is also probably due partly to a desire to meet the adequacy requirements of the E.U. Directive Articles 25–26. In some cases, stimulus is also provided by recent first-hand experience of mass oppression. The Republic of South Africa has come furthest along the path to establishing a comprehensive legal regime on data privacy. 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,[157] and work is proceeding on a bill for separate data privacy legislation.[158] Kenya is also drafting a new Constitution containing similar rights as found in the South African Constitution.[159]

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).[160]

Further complicating matters is that each country's data privacy regime consists of more than formal legal rules. While the latter, together with formal oversight mechanisms, are important constituents of a data privacy regime, they

---

156 *See* Pedersen, A., *India plans EU-style data law*, Privacy Laws & Business 2003, Issue 68, p. 1, 3.

157 *See* The Promotion of Access to Information Act 2 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.

158 *See* Currie and Klaaren, *supra* note 157, p. 11, 18. *See* also Electronic Privacy Information Centre and Privacy International, *supra* note 64, p. 450.

159 *See* sections 14 (right of privacy) and 47 (rights of information access and rectification) of the Draft Bill for The Constitution of the Republic of Kenya (version of 27th September 2002).

160 This classification of criteria is based on Bennett and Raab, *supra* note 37, p. 193 *et seq*.

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 privacy 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.[161] 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 privacy agency with strong formal powers will necessarily have greater success in fulfilling its objectives than an agency with weaker formal powers.[162]

Yet another complicating element is that the regulatory approach of many data privacy 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.[163] 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.[164]

These problems notwithstanding, a large degree of consensus exists amongst experts in the field regarding the relative strengths of certain data privacy regimes. Part of this consensus is a view that the U.S. data privacy 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 privacy 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".[165] The major reasons for this finding are the lack of a U.S. federal data privacy agency, together with the paucity of comprehensive data privacy 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

---

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

162 Again, *see* Flaherty, *supra* note 161. Note particularly Flaherty's finding that the German Federal Data Protection Commissioner (Bundesdatenschutzbeauftragter) – which has only advisory powers – had, at least up until the late 1980s, 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.

163 *Id.*

164 For further discussion on the difficulties of comparative assessment of data privacy regimes, *see* Bennett and Raab, *supra* note 37, 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.

165 Flaherty, *supra* note 161, p. 305.

analyses.[166] 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.[167]

By contrast, the German data privacy regime is often viewed as one of the most successful.[168] 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.[169] Another such feature is extensive encouragement of "systemic data protection" ("Systemdatenschutz"); i.e., integration of data privacy concerns in the design and development of information systems architecture.[170] 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 privacy issues, the relatively conformist, legalistic nature of German administrative and corporate cultures, the strong, persuasive personalities of the men who have been appointed data privacy commissioners, together with the considerable talents of their staff.[171] Nevertheless, the data privacy regime in Germany does have weak points. One weakness is the Federal Data Protection Commissioner's lack of competence to issue legally binding orders – a feature that is arguably at odds with the thrust of Directive 95/46/EC. Another, more significant, weakness is the sheer mass of rules on data privacy; the regulatory framework is so dense as to be confusing, non-transparent and unwieldy.[172] These weaknesses mean that, despite its relative success, the German regime still falls short of meeting its policy objectives.

Data privacy regimes in most other, if not all, jurisdictions display a similar shortfall. European regimes in general are a case in point. There is sporadic evidence that many of these 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.[173] More significantly, the European Commission has

---

166 The most extensive being Schwartz and Reidenberg, *supra* note 11 – *see* especially their conclusions at p. 379–96.

167 For a particularly damming critique of the U.S. judiciary's response to privacy litigation, *see* Anderson, D.A., *The Failure of American Privacy Law*, in Markesinis, B.S. (ed.), Protecting Privacy, Oxford University Press, Oxford 1999, p. 139–167.

168 *See, e.g.*, Flaherty, *supra* note 161, especially p. 21–22.

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

170 *See* particularly Federal Data Protection Act, sections 3a, 9; Federal Teleservices Data Protection Act of 1997 (*Gesetz über den Datenschutz bei Telediensten vom 22. juli 1997*) (as amended in 2001). For further discussion, *see* Bygrave, *supra* note 16, particularly p. 346, 371.

171 *See* generally Flaherty, *supra* note 161, Part 1.

172 *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, "http://www.bmi.bund.de/downloadde/11659/Download.pdf" (last accessed 20th July 2004).

173 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

recently found that while the E.U. Directive (95/46/EC) has created a "high level" of data privacy in Europe, implementation of the Directive is afflicted by major problems.[174] Not only has national transposition of the Directive often been slow,[175] there appear to be – even after transposition – low levels of enforcement, compliance and awareness with respect to the national regimes. Data privacy agencies in Europe have been found, in general, to be under-resourced, leading in turn to under-resourcing of enforcement efforts. Concomitantly, the Commission has found that compliance by data controllers is "very patchy", while data subjects have low awareness of their data protection rights.[176] Moreover, there remain differences between the various national laws which run counter to the harmonising objective of the Directive.[177] Particularly problematic from an international perspective, is that E.U. member states' respective implementations of Articles 25–26 in the Directive has been very broadly divergent; indeed, in many cases, it has been inconsistent with the Directive. Further, the Commission has found that a 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 privacy regimes *generally*. One line of criticism concerns the regimes' underdevelopment of a systemic focus – as manifested, for instance, in the paucity of direct legislative encouragement for privacy-enhancing technologies.[178] 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 privacy norms. This situation not only results in scarcity of authoritative guidance on the proper interpretation of the relevant

---

policies. *See* Consumers International (Scribbins, K.), *Privacy@net: An international comparative study of consumer privacy on the internet*, "http://www.consumersinternational.org/document_store/Doc30.pdf" (last accessed 20th July 2004). *See* too results of a more recent survey published in April 2003 by World IT Lawyers. This survey canvassed 420 commercial websites across seven countries (France, Germany, Netherlands, Portugal, Switzerland, Spain, U.K.) and found that approximately half of these sites did not display a privacy policy: *see* Broersma, M., *UK web sites fare badly on consumer rights*, ZDNet UK, 30th April 2003, "http://news.zdnet.co.uk/business/0,39020645,2134138,00.htm" (last visited 20th July 2004).

174 E.C. Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, Brussels, 15th May 2003, available at "http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf" (last accessed 20th July 2004).

175 Several E.U. member states have been tardy in transposing the Directive into national law, the principal laggards being France, Ireland, Luxembourg and Germany. Further on implementation status with respect to the Directive, *see* "http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm" (last visited 20th July 2004).

176 European citizens' poor awareness on this point is further evidenced by a Eurobarometer survey carried out in September 2003 on behalf of the Commission. See the results at <http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf> (last accessed 20th July 2004).

177 *See* also Korff, *supra* note 130; Charlesworth, A., *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?*, Hastings Law Journal 2003, vol. 54, p. 931–969.

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

legislation but contributes to the marginalisation of data privacy as a field of law.[179]

The potentially most damaging line of criticism is that data privacy 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 privacy 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.[180] 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.[181] 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 long-standing, widespread concern to protect privacy and related interests, particularly in the face of developments in I.C.T. Regulatory responses to this concern in the form of data privacy 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 privacy laws in the various countries 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 privacy regimes. It is pertinent, therefore, to conclude with some brief comments about the chances of achieving greater harmonisation of regimes across the globe. In my view, it is extremely doubtful that we will see, at least in the short term, major progress with respect to harmonisation at the global level.[182] This is due not simply to the strength of ingrained ideological/cultural differences around the world but also to the lack of a sufficiently strong, dynamic and representative international body to bridge

---

179 *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.

180 *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 160.

181 *See, e.g.*, Bygrave, *supra* note 16, chapter 18 and examples cited therein; *see* also Flaherty, *supra* note 161, particularly Part 1.

182 Further on the problems of achieving international harmonization on data privacy issues, *see* especially Reidenberg, *supra* n. 61.

those differences. The World Trade Organisation (W.T.O.) is occasionally touted as such a body. Yet its ability to negotiate a broadly acceptable agreement on data privacy issues will be hampered by its commercial bias. Its ability to negotiate such an agreement quickly and efficiently is also in doubt given its apparent tardiness during the Doha Round of negotiations in crystallising policy with respect to electronic commerce.

As for harmonisation efforts at the regional level, the track record of A.P.E.C. is yet to be 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 privacy regimes of non-European states in line with its preferred model. This is partly because of the recent emergence of A.P.E.C. as a potential competitor in the role of data privacy "superpower". Yet it is also because of the weak implementation of Articles 25–26 in the E.C. Directive. How those rules are implemented, constitutes an important litmus test for the Directive's international credibility and success. Unfortunately for the Directive, its regime for transborder data flow to third countries seems to be 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.