Data Privacy Law

An International Perspective

LEE A. BYGRAVE

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

First Edition published in 2014

Impression: 1

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2013946837

ISBN 978–0–19–967555–5

Printed in Great Britain by
CPI Group (UK) Ltd, Croydon, CR0 4YY

Contents

1

Data Privacy Law in Context

A. Definition of Field

Data privacy law specifically regulates all or most stages in the processing of certain kinds of data. It accordingly addresses the ways in which data is gathered, registered, stored, exploited, and disseminated. Not all types of data fall within its ambit. Its rules typically apply only to data that relates to, and permits identification of, individual physical/natural persons (hereinafter also termed simply 'individuals'). In rare cases, its rules apply also to data concerning corporations and other legal/juristic persons, along with organized collective entities more generally.[1] Formally, data privacy law is aimed primarily at safeguarding certain interests and rights of individuals in their role as data subjects—that is, when data about them is processed by others. These interests and rights are usually expressed in terms of privacy, and sometimes in terms of autonomy or integrity.

The central rules of data privacy law embody a set of largely procedural principles. The core of these principles may be summed up as follows:[2]

- personal data should be collected by fair and lawful means (principle of fair and lawful processing);
- the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered and further processed (principle of minimality);
- personal data should be collected for specified, legitimate purposes, and not used in ways that are incompatible with those purposes (principle of purpose limitation);
- personal data should be relevant, accurate, and complete in relation to the purposes for which it is processed (principle of data quality);
- personal data should be protected against unauthorized attempts to disclose, delete, change, or exploit it (principle of data security);

[1] See further Ch 4 (section C(6)).

[2] For elaboration, see Ch 5.

- processing of personal data should be transparent to, and capable of being influenced by, the data subject (principle of data subject influence).

These are not the only principles found in data privacy law but they are central to it. More general principles not specific to the field come into play too. The proportionality principle is an example, particularly with respect to EU law.[3] Elements of the above principles and some of the rights to which they give rise are also found outside data privacy law, for instance in legislation on freedom of information (FOI)—that is, legislation enabling public access to government-held information.[4] Yet only legal instruments embracing all or most of the above principles are commonly considered as data privacy law—a line also taken in this book.

Data privacy is not fully commensurate with data security. This should be obvious from the above-listed principles but bears emphasis particularly since the European nomenclature for the field ('data protection') appears closely related to data security and has been conflated with the latter.[5] While data security is a component of a data privacy (or data protection) regime, the latter embraces other rules and measures too. At the same time, data security on its own may serve a broader range of concerns than data privacy. Whereas a primary goal of data privacy is protection of data subjects' privacy-related interests, data security as such can also be aimed at safeguarding the interests of controllers, processors, and users of all kinds of data (not just personal data) in the name of, say, national security or administrative efficiency. The same applies with the overlapping areas of information security and information systems security. The security measures are mainly directed towards ensuring that data is processed in accordance with the expectations of those who steer or use a given information system. The chief sub-goals for these measures are maintenance of the confidentiality, integrity/quality, and availability of information in an information system as well as appropriate protection of the system itself.[6] In many instances, these measures may serve to promote data privacy, but they can obviously come into conflict with the latter as well.

[3] See further Ch 5 (section C).

[4] See further section C.

[5] For an example from the field of database management, see CJ Date, *An Introduction to Database Systems* (6th edn, Addison-Wesley 1995) 373. Raab claims that such conflation is 'frequently encountered in organizational circles, including policing': CD Raab, 'Police Cooperation: The Prospects for Privacy' in Malcolm Andersen and Monica den Boer (eds), *Policing across National Boundaries* (Pinter 1994) 121, 124.

[6] See eg, Nordic Council of Ministers, *Information Security in Nordic Countries*, Nordiske Seminar-og Arbejdsrapporter 1993: 613 (Nordic Council of Ministers 1994) 12.

Data privacy (or data protection) is also not fully commensurate with privacy, at least if the latter is defined in terms of non-interference, limited accessibility, or information control.[7] Again this should be obvious from the principles listed earlier, but bears emphasis due to the tendency in some non-European countries to call the field simply 'privacy law'. In some respects, data privacy canvasses more than what are typically regarded as privacy concerns.[8] The rules aimed at ensuring adequate data quality are an example in point. In other respects, data privacy encompasses less than privacy per se. The latter has spatial, bodily, and perhaps psychological dimensions that are usually not directly addressed by data privacy law.[9]

Four more distinguishing features of the field are worth noting at this preliminary stage. The first is that data privacy law is largely statutory. This is not to say that case law or various forms of 'soft law', such as guidelines, recommendations, and codes of conduct, fall outside the field, but the central rules are usually laid down in legislation. In many jurisdictions, this legislation has been shaped, construed, and applied with little involvement from the judiciary.[10]

The second feature is that data privacy statutes usually establish special independent bodies to oversee their implementation. These bodies are commonly termed 'data protection authorities' or 'privacy commission(er)s'. In keeping with my choice of nomenclature for the legal field concerned, they are herein termed 'data privacy agencies' (DPAs). These bodies are usually given broad, discretionary powers to monitor and regulate the data-processing activities of organizations in the public and private sectors. Their functions typically extend to handling complaints, giving advice, and raising public awareness of data privacy.[11]

The third feature is that data privacy statutes often take the form of so-called 'framework' laws. Rather than stipulating in casuistic fashion detailed rules on data processing, the legislation tends to set down rather diffusely formulated, general rules for such processing, and provide for the subsequent development of more detailed rules as the need arises. This is symptomatic of legislators' desire for regulatory flexibility in the face of technological complexity and change, together with uncertainty over the nature of the interests to be

[7] On various common conceptualizations of 'privacy', see section F and references cited therein.

[8] See further Ch 4 (section B).

[9] For discussion of some of those dimensions and their interaction with data privacy law, see LA Bygrave, 'The Body as Data? Biobank Regulation via the "Back Door" of Data Protection Law' (2010) 2 Law, Innovation and Technology 1–7.

[10] Further on the role of the judiciary, see Ch 6 (section B).

[11] See further Ch 6 (section A).

protected.[12] Primary responsibility for developing more specific rules is often given to the respective DPA.

The second and third listed features underscore the fourth, which is that DPAs frequently play a lead role in laying down how data privacy law is understood and applied, even in contexts where their views on point are only advisory. In many countries, such as Australia, Denmark, France, NZ, Norway, and the UK, they have been able to play this role with little corrective input from the courts.

Having DPAs play that role carries obvious advantages—they are, after all, the appointed experts in the field. Yet there is also a risk that DPAs construe data privacy legislation in ways that further the cause of data privacy at the expense of other factors that require equal or greater weighting as a matter of *lex lata*. That risk is acute when promotion of data privacy is central to a DPA's formal remit. The judiciary, approaching the legislation with relatively fresh eyes and formally unencumbered by a pro-privacy mandate, will tend to be better able to resist such bias. Yet courts' frequent lack of familiarity with the legislation, combined with the time pressures of litigation, can result in their failing to appreciate the complexities of the legislation in ways that undermine the correctness of their judgments.[13] There is accordingly good reason to approach both administrative practice and case law in the field with a critical eye.

B. Significance of Field

Processing personal data has always been integral to human interaction. It has long been central to the tasks of governmental agencies, especially since the emergence of the welfare state. Yet it has assumed unprecedented proportions and significance in our current 'information society', particularly as a source of economic productivity.[14] Personal data has thus been termed 'the new oil'.[15] A rapidly growing market exists in which personal data as such is traded

[12] See eg, H Burkert, 'The Law of Information Technology—Basic Concepts' (1988) Datenschutz und Datensicherheit 383, 384–5.

[13] See eg, Ch 5 (n 60).

[14] M Castells, *The Rise of the Network Society* (Blackwell 1996); D Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting* (Basic Books 1973).

[15] World Economic Forum (WEF), *Personal Data: The Emergence of a New Asset Class* (WEF, January 2011), available at: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Brown and Marsden, though, aptly suggest that personal data ought to be viewed rather as the new 'silk', at least in the context of the Internet: I Brown and CT Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013) 184 ('Personal data accumulate with the individual's treks into cyberspace, and therefore a better metaphor is silk, woven into the tapestry of the user's online personality').

and employed as the basis for marketing and control strategies. Consider, for instance, the burgeoning trade in customer lists as commodities in their own right.[16] Consider also how much of the 'Internet economy' is fuelled by, and premised on, persons supplying data about themselves (wittingly or unwittingly) in exchange for otherwise ostensibly free online services. At the same time, the informational appetite of public sector agencies grows too. This is most obvious (though often hard to document reliably) with the surveillance schemes of national security and police agencies. Consider, for instance, the expansive ambitions behind some such schemes initiated as part of the ongoing 'war on terror'.[17] The delivery of services by other government agencies involves intensified processing of personal data as well. This intensification has traditionally been justified in terms of ensuring that services flow only to those citizens who need or legally qualify for them.[18] In recent years, fiscal imperatives have also played a prominent role in justifying agencies' push for more fine-grained knowledge of their 'clients' and 'customers'.[19]

It is in light of all these developments that the broad significance of data privacy law becomes apparent. Because it seeks to regulate directly the exploitation of personal data, such law has the potential to interfere (positively or negatively) with many of the processes mentioned. It can thereby generate considerable administrative, commercial, political, or social costs (or gains). This potential is augmented by the considerable powers that DPAs are often given to steer data-processing activities in both the public and private sectors.

Data privacy law is also important on the normative plane. In the 'information society', its principles and ideals are amongst the central counterweights to technocratic imperatives, such as increased organizational efficiency and maximization of financial profit. This is not to suggest that data privacy law is intrinsically opposed to such imperatives; in some respects, it aids their realization. Yet it also emphasizes a need to take account of other interests, thus enriching our normative sphere.

The broad significance of data privacy law is partly reflected in the heightened focus on rights to privacy and private life, with which such law is closely

[16] E Novak, N Sinha, and O Gandy, 'The Value of Your Name' (1990) 12 Media, Culture & Society 525.

[17] See eg, S Gorman, 'NSA's Domestic Spying Grows As Agency Sweeps Up Data', *Wall Street Journal*, 10 March 2008, A1; G Greenwald and E MacAskill, 'NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveal', *The Guardian*, 6 June 2013, available at: <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

[18] See eg, J Rule, D McAdam, L Stearns, and D Uglow, *The Politics of Privacy: Planning for Personal Data Systems As Powerful Technologies* (Elsevier 1980) 43, 45, 48–9.

[19] D Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Polity Press 1994) 88ff and references cited therein.

connected. Frowein and Peukert claim that the right to private life has constituted the major challenge for liberal states' legal systems during the latter half of the twentieth century.[20] The claim is somewhat exaggerated yet has a kernel of truth. Debate over privacy rights has assumed a prominent place in many legal systems. For instance, the right to respect for private life set down in Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[21] has become one of the most frequently contested rights in case law pursuant to the Convention.[22] This is symptomatic of the gradual expansion of the public sphere into previously private domains—a development partly brought on by organizations' growing informational appetite. Privacy rights are being used to shield persons from the detrimental effects of this development.

The broad significance of data privacy law is further reflected in the controversy frequently embroiling its gestation. The birth of the Federal Republic of Germany's first Federal Data Protection Act was well nigh the hitherto most complicated, drawn out, and contentious legislative process in the country's history.[23] Subsequent revision of that Act and its replacement by new legislation was also far from 'short and sweet'.[24] In Finland, work on drafting the country's first main data privacy law—the Personal Data Registers Act 1987[25]—took over fifteen years and was frequently paralysed by political conflict.[26] Initial enactment of similar legislation in many other jurisdictions, such as the UK, Australia, and the Netherlands, was also controversial.[27] At the supranational level, the EU's drafting and adoption of the Data Protection

[20] JA Frowein and W Peukert, *Europäische MenschenRechtsKonvention: EMRK-Kommentar* (2nd edn, NP Engel 1996) 338.

[21] Opened for signature 4 November 1950; in force 3 September 1953; ETS 5 (hereinafter also 'European Convention on Human Rights' or 'ECHR').

[22] For an overview of this case law, see DJ Harris, M O'Boyle, E Bates, and C Buckley, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (2nd edn, OUP 2009) chs 8–9.

[23] S Simitis, 'Einleitung' in S Simitis, U Dammann, O Mallmann, and HJ Reh (eds), *Kommentar zum Bundesdatenschutzgesetz* (3rd edn, Nomos 1981) 69. Further on the process in English, see eg, AL Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press 2008) 63–9.

[24] S Simitis, 'Einleitung' in S Simitis (ed), *Bundesdatenschutzgesetz* (7th edn, Nomos 2011) 97–115.

[25] *Henkilörekisterilaki/Personregisterlag* (FFS 471/87); repealed and replaced by the Personal Data Act 1999 (*Henkilötietolaki/Personuppgiftslag* (FFS 523/99)).

[26] See eg, J Kuopos, 'Finland' in D Campbell and J Fisher (eds), *Data Transmission and Privacy* (Martinus Nijhoff 1994) 161, 162.

[27] Regarding the UK, see eg, CJ Bennett, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992) 82–94, 209ff. In relation to Australia, see eg, LA Bygrave, 'The Privacy Act 1988 (Cth): A Study in the Protection of Privacy and the Protection of Political Power' (1990) 19 Federal L Rev 128, 137ff. Regarding the Netherlands, see eg, VA de Pous, 'Dutch Privacy Bill Again Delayed' (1988) 11 Transnational Data Report, no. 10, 6–7.

Directive (95/46/EC)[28] took over five years and was subject to hefty debate and frenetic lobbying.[29] The legislative process currently in train with the proposal for a new EU Regulation in the field bears similar hallmarks.[30]

Although much of the controversy afflicting these legislative processes springs from the laws' putative potential to impinge negatively upon the ways in which organizations function, other factors have sometimes played a role too. For instance, the constitutional system of the UK along with its customary statutory drafting techniques hampered the initial adoption of data privacy legislation there.[31]

The legislative controversy in this area has sometimes been channelled along the traditional, Left–Right axis of political conflict—the case, for example, in Finland.[32] Yet concern for data privacy generally spans a broad range of political ideologies. In the words of Bennett:

> [t]he issue [of data privacy] is so sufficiently broad that it can encompass a variety of different positions, from the civil libertarian who demands constraints on overzealous law enforcement to the conservative business group that wants tax data to be kept confidential. The issue tends to pose a dilemma for democratic socialist parties in particular; it exposes a tension between the welfare statism of the old Left, which relies on a sacrifice of individual privacy for the collective benefit, and the more antistatist individualism of the new Left. Thus below the broad liberal democratic concern for individualism and human dignity lies a complex and often contradictory set of positions. […] The ideological foundations of the issue are inherently ambiguous because privacy and data protection do not stir partisan emotion until the debate centers on particular information in specific contexts. We then find a complexity of cross-cutting concerns.[33]

[28] 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 [1995] OJ L281/31.

[29] See eg, N Platten, 'Background to and History of the Directive' in D Bainbridge (ed), *EC Data Protection Directive* (Butterworths 1996) 23–32; S Simitis, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data' (1995) 80 Iowa L Rev 445. For a detailed description of the lobbying campaigns, see PM Regan, 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics' in CJ Bennett and R Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press 1999) 199.

[30] See eg, C Burton, C Kuner, and A Pateraki, 'The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report' *Bloomberg BNA Privacy and Security Law Report* (21 January 2013) 1. The proposed Regulation is dealt with in Ch 2 (section E(3)).

[31] PM Regan, 'Protecting Privacy and Controlling Bureaucracies: Constraints of British Constitutional Principles' (1990) 3 *Governance* 33; M Stallworthy, 'Data Protection: Regulation in a Deregulatory State' (1990) 11 Statute L Rev 130, 134ff.

[32] A Saarenpää, 'Data Protection: In Pursuit of Information. Some Background to, and Implementations of, Data Protection in Finland' (1997) 11 Intl Rev of Law, Computers & Technology 47, 48.

[33] Bennett (n 27) 147.

Its broad normative and practical significance notwithstanding, data privacy law is not the only set of legal rules impacting on organizations' informational appetite. Consider, for instance, employers' ability to engage in employee surveillance: in addition to data privacy law, rules in both statute and case law dealing specifically with labour relations may also have an impact, as may various contracts. For example, the European Social Charter[34] contains general provisions establishing workers' rights to 'just conditions of work' (Article 2), to 'information and consultation' by and from employers (Article 21), to co-determination of working conditions (Article 22), and to 'dignity at work' (Article 26). Each of these rights indirectly restricts employers' monitoring of their employees. As for contracts, collective bargaining agreements or collective employment agreements reached between employers and trade unions may contain rules limiting workplace surveillance. Further, the terms of the individual contract of employment may be important in determining how data on an employee is collected by their employer and the uses to which that data may be put, particularly in the absence of further consent by the employee.

C. Catalysts and Origins

The aetiology of data privacy law is complex. This section provides only a short, simplified explication.[35] In a nutshell, data privacy law results from an attempt to secure the privacy, autonomy, and integrity of individuals and thereby the bases for democratic, pluralist society in the face of massive growth in the amount of personal data gathered and shared by organizations. Other law has been perceived as unable to adequately secure these interests. Data privacy law has thus been created to fill the breach.

Looking more closely at that account, we see three categories of factors behind the emergence of data privacy law: (i) technological and organizational developments in the processing of personal data; (ii) fears about these developments; and (iii) other legal rules. Each of these categories is elaborated in the following.

[34] First version (ETS 35) opened for signature 18 October 1961; in force 26 February 1965. Revised version (ETS 163) opened for signature 3 May 1996; in force 1 July 1999.

[35] A fuller explanation—upon which this account builds—is given in LA Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002) ch 6.

1. Technological and organizational developments

The first category embraces a broad range of developments in data processing. They are developments facilitated and, to some extent, driven by the growing power of information and communication technology (ICT). Yet their catalysts are also economic, social, and political. They are linked with efforts to enhance organizational efficiency, profitability, prestige, control, and service. Such efforts are symptomatic of a deep-seated concern for reflexivity and rationalization.

The most important developments are, firstly, greater dissemination, use, and re-use of personal data across organizational boundaries and, secondly, replacement or augmentation of manual control mechanisms by automated mechanisms. Corollaries of these trends include increases in:

- use of data for purposes other than the purposes for which it was originally collected ('re-purposing');
- potential for misinterpretation and misapplication of data and for dissemination of invalid or misleading data;
- automatization of organizational decision-making processes;
- the blurring and dissolution of transactional contours.

These developments result in information systems of growing complexity and diminishing transparency, at least from the perspective of individuals in their role as data subjects. At the same time, individuals are rendered increasingly transparent for the various organizations with whom they deal. An evermore pervasive, subtle, and finely spun web of mechanisms monitor and shape their activities. Individuals additionally risk being assessed or interfered with on the basis of data about them that is incorrect or otherwise of poor quality.

All of these developments figure in the discourse out of which data privacy law has emerged, though they are often less abstract than the above depiction suggests.[36] An early manifestation of them (or, more accurately, elements of them) was government initiatives during the 1960s and early 1970s to

[36] In the USA, see particularly, AF Westin, *Privacy and Freedom* (Atheneum 1967) chs 7 and 12; AR Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (University of Michigan Press 1971) chs I–III. In the UK, see eg, M Warner and M Stone, *The Databank Society: Organizations, Computers, and Social Freedom* (Allen & Unwin 1970); P Sieghart, *Privacy and Computers* (Latimer 1976) esp. chs 2–3. In Norway, see eg, E Samuelsen, *Statlige databanker og personlighetsvern* (Universitetsforlaget 1972) 11–12 and ch 4; *Offentlige persondatasystem og personvern*, NOU 1975:10 esp. 10ff; *Persondata og personvern*, NOU 1974:22 esp. 6–7, 28ff. In Sweden, see particularly *Data och integritet*, SOU 1972:47 esp. 30–2, and chs 3–7. In Switzerland, see esp. *Botschaft zum Bundesgesetz über den Datenschutz vom 23.3.1988* 4–5. For a general overview of this discourse and the issues motivating it, see Bennett (n 27) ch 2.

establish centralized population databases.[37] Government plans to conduct comprehensive national population censuses were another manifestation,[38] as were efforts to introduce common criteria (for example, multi-purpose Personal Identification Numbers (PINs)) for matching stored data.[39] These and similar schemes provided much of the fuel for the public debates that helped set in train the enactment of early data privacy legislation.[40]

2. Fears

The debates have expressed a congeries of fears clustered about three interrelated themes: (i) increasing transparency, disorientation, and disempowerment of individuals; (ii) loss of control over technology; and (iii) dehumanization of societal processes. The central fear relates primarily to the first-mentioned theme: it is that these developments, if unchecked, will undermine the foundations of democratic, pluralist society. Experiences of systematic authoritarian repression (for example, Nazism) and attempts to subvert political due process (for example, the Watergate scandal) have fed this fear, as has dystopian literature (for example, Orwell's *Nineteen Eighty-Four*). The pervasiveness of the fear reflects growing distrust of organizations and technology. This growth in distrust reflects, in turn, a general societal trend whereby human action is increasingly weighed down by awareness of risk.[41]

Another class of fears has also played a role in the adoption of data privacy codes, though *after* these codes' initial enactment in the 1970s. The fears are primarily economic in nature and shared by governments and businesses. One anxiety is that data privacy law will unduly impede transborder flow of data. This anxiety arose because the nascent national data privacy laws of Europe restricted flow of personal data to countries not offering levels of data privacy similar to the 'exporting' jurisdiction. As elaborated in Chapter 6,

[37] A salient example was the proposal in the mid-1960s to set up a National Data Center in the USA which would consolidate in one database all information on US citizens held by federal government agencies: see further Miller (n 36) 54–67. Another was the implementation in France of a computerized system (SAFARI—Système automatisé pour les fichiers administratifs et le répertoire des individus) which was to aggregate data on French citizens using their social security numbers as a key for the matching: see further A Vitalis, 'France' in JB Rule and G Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar 2008) 107.

[38] The most high profile of these plans was embodied in the German federal Census Act 1983—legislation that triggered a famous decision by the German Federal Constitutional Court on the constitutional right to 'informational self-determination'. See further Ch 6 (n 45).

[39] A prominent and highly controversial example being the 'Australia Card' scheme of 1987: see further G Greenleaf, 'Australia' in JB Rule and G Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar 2008) 141–2.

[40] See too generally Bennett (n 27) 46–53.

[41] For seminal analysis on point, see U Beck, *Risk Society: Towards a New Modernity* (Sage 1992).

such restrictions have become an integral element of numerous data privacy regimes. The principal international codes in the field have all been introduced partly in order to minimize the deleterious impact that such restrictions could exercise on international commerce and freedom of expression. The other fear concerns the possibility that, in the absence of data privacy law, the general populace will lack confidence to participate in commerce, particularly as consumers/prosumers. Enactment of data privacy law can thus be partly explained as an effort to shore up public trust in the way organizations process personal data.[42]

3. Legal factors

Data privacy legislation would obviously not have been enacted but for perceived failings in the ability of pre-existing laws to tackle adequately the problems arising out of the earlier mentioned two categories of factors. To some extent, pre-existing laws were perceived as *aggravating* these problems. In Sweden, for example, its constitutionally entrenched, long-standing, and liberal freedom of information (FOI) regime was regarded as particularly problematic for privacy with the advent of computerization. The latter meant that the exercise of FOI rights could lead to relatively fast and easy dissemination of large amounts of personal data. Enactment of Sweden's first data privacy legislation has accordingly been described as a qualification of the principle of freedom of information, made in recognition of the threat to personal privacy raised by the age of computers'.[43]

Pre-existing law has also shaped data privacy law in a more positive way, by providing normative foundations or sources of inspiration for it. Statutory rules and case law laying down rights to privacy or protection of personality are the most obvious instances.[44] Rules on defamation are also pertinent. All of these rules prefigure the basic thrust of data privacy law in that they restrict various kinds of behaviour, including certain ways of processing information, in order to protect the integrity, autonomy, dignity, or privacy of individuals.

Less obvious but perhaps more important in this respect is the role played by administrative law together with general doctrines on the rule of law. Traditional rules on due administrative process embody principles that are

[42] See further eg, H Burkert, 'Systemvertrauen: Ein Versuch über einige Zusammenhänge zwischen Karte und Datenschutz' (1991) *á la Card Euro-Journal*, no. 1, 52.

[43] DH Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press 1989) 99.

[44] For Norwegian examples, see Bygrave (n 35) 126–7.

precursors to some of the central data privacy principles. Strong links exist between the principles of data quality and data subject influence in data privacy law on the one hand and, on the other hand, the general requirements of procedural fairness ('natural justice') under administrative law. Central amongst those requirements are that government agencies base their decisions on relevant evidence, be unbiased in the matters to be determined, and give persons who may be adversely affected by the decisions the opportunity to be heard. Moreover, the right under data privacy law of data subjects to access data on themselves kept by others parallels the information access rights under FOI legislation. This is not to say that these areas of law are fully commensurate with each other. In contrast to data privacy law, FOI legislation usually allows persons access to both personal and non-personal information held by government and, concomitantly, to information not just on themselves but other persons.[45] Thus, exercise of FOI rights can come into conflict with data privacy.[46] Whereas administrative law is traditionally limited to regulating the relationship between state organs and citizens, data privacy law often regulates the relationship between private organizations and individuals as well. And whereas large parts of administrative law focus on specific decision-making schemes, data privacy law focuses mainly on the processing of personal data, which is not necessarily tied to a specific decisional process.

Law and doctrine on human rights also pervade data privacy law. Indeed, as elaborated in the next chapter, they are now generally regarded as providing the principal normative basis for such law. Concomitantly, much of the latter is now seen as both an expression and specialized branch of the former. This is especially noteworthy as the links between data privacy and human rights were less recognized when data privacy legislation first emerged. In Norway, for instance, enactment of its first data privacy statute in 1978 was accompanied by considerable awareness of the close similarities with administrative law, whilst the connection to human rights was downplayed.[47] Also noteworthy is that the Council of Europe began work on drafting its early data privacy codes due to a perception that the ECHR did not provide

[45] Further on the differences and similarities between FOI and data privacy law, see H Burkert, 'Data Protection and Access to Data' in P Seipel (ed), *From Data Protection to Knowledge Machines* (Kluwer Law & Taxation Publishers 1990) 49; European Data Protection Supervisor (EDPS), *Public Access to Documents and Data Protection* (EC 2005).

[46] See eg, Ch 4 (n 87).

[47] See eg, J Bing, 'Information Law?' (1982) 2 J of Law and Media Practice 219, 232 (claiming that Norwegian and other European data privacy laws are 'more closely related to the law of public administration than to the law of individual liberties'). See further Bygrave (n 35) 127–8 and references cited therein.

adequate protection for individuals in the face of computerized processing of personal data, particularly in the private sector.[48] Case law of the ECtHR since then has shown that the ECHR is a powerful data privacy instrument in its own right.[49] Other courts and lawmakers increasingly use that jurisprudence as benchmarks for developing, interpreting, and applying data privacy instruments.[50]

Numerous other areas of law have helped inspire or support data privacy law. These include rules in labour law on worker co-determination and fair workplace practices. For example, the first influential set of data privacy principles drafted in the USA—the 'Fair Information Practices' drawn up in 1973 by the federal Department of Health, Education and Welfare (DHEW)[51]—are said to have been inspired by a code of fair labour practices.[52]

Law on intellectual property rights (IPR) is a further case in point. Doctrines on copyright have been used to help ground a right to privacy, which has, in turn, helped ground data privacy law, while privacy doctrines have been used to help ground aspects of copyright.[53] The two sets of rights have also worked hand in hand on a more practical plane. For instance, the publication of certain film material in which persons are portrayed is often restricted under copyright law.[54] Nonetheless, the relationship of copyright and data privacy has grown far less cordial over the last 15 years. In their battle against digital piracy, IPR-holders have frequently been frustrated by data privacy law, particularly for hindering their ability to identify the putative pirates. A remarkably large part of recent litigation on data privacy law has been initiated by IPR-holders seeking to curtail such hindrances.[55]

[48] See eg, FW Hondius, *Emerging Data Protection in Europe* (North Holland Publishing Company 1975) 63ff and references cited therein.

[49] See further Ch 2 (section I(2)).

[50] See eg, Ch 2 (n 109).

[51] US Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens* (US Government Printing Office 1973) 41.

[52] WH Ware, 'A Historical Note' in US Department of Health and Human Services, Task Force on Privacy, *Health Records: Social Needs and Personal Privacy* (Conference Proceedings) (US Government Printing Office 1993) Addendum A, 50.

[53] Famous examples being S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 Harvard L Rev 193, 198 (arguing, inter alia, that common law protection of intellectual, artistic, and literary property is based upon a broader principle of protection of privacy and personality); J Kohler, 'Das Autorrecht' (1880) 18 Jherings Jahrbücher für die Dogmatik des Bürgerliches Rechts 128 (basing authors' moral rights partly on the notion that the authors' works originate within their private sphere).

[54] See eg, UK Copyright, Designs and Patents Act 1988 s 85(1); Australia's federal Copyright Act 1968 s 35(5); Norway's Intellectual Property Act 1961 (*lov om opphavsrett til åndsverk mv 12 mai 1961 nr 2*) s 45c.

[55] See further LA Bygrave, 'Data Protection versus Copyright' in DJB Svantesson and S Greenstein (eds), *Internationalisation of Law in the Digital Information Society: Nordic Yearbook of Law and Informatics 2010–2012* (Ex Tuto Publishing 2013) 55.

Turning to doctrines on property rights more generally, these have undoubtedly played a part in inspiring data privacy law. However, gauging the extent of this role is difficult. Much depends on how property rights are defined. They can be defined so generally as to to form the basis for large tracts of the legal system.[56] If defined more narrowly as conferring a legally enforceable claim on the rights holder to exclude others from utilizing a particular object or thing, we can still discern some reflection of such rights in the requirement under data privacy law that processing of personal data is conditional on the consent of the data subject(s).[57] However, data privacy law frequently permits circumvention of that requirement so the resultant level of data 'ownership' often has little real traction.[58] There tend to be few, if any, other obvious manifestations of property rights doctrines in data privacy statutes or their *travaux préparatoires*. Some of the early and influential contributors to the discourse out of which data privacy law emerged championed property rights as a foundation for such law.[59] However, others amongst them rejected this line.[60] Subsequent advancement of a property rights approach tends to come from US scholars,[61] although the most recent and thorough advocacy of such an approach comes from a European.[62] Nonetheless, the majority of contributors to the debate, especially in Europe, reject property rights doctrines as a desirable basis for data privacy law.[63]

[56] See eg, Warren and Brandeis (n 53) 211 ('The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested').

[57] See further D Elgesem, 'Remarks on the Right of Data Protection' in J Bing and O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (TANO 1995) 83, 90ff.

[58] See further Ch 5 (section F).

[59] See eg, Westin (n 36) 324–5.

[60] See eg, Miller (n 36) 211ff.

[61] See eg, KC Laudon, 'Markets and Privacy' (1996) 39 Communications of the ACM 92; L Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 159–62; JB Rule and L Hunter, 'Towards Property Rights in Personal Data' in CJ Bennett and R Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999) 168–81; JB Rule, *Privacy in Peril* (OUP 2007) 196–8. Cf PM Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard L Rev 2056 (critically discussing various objections to a property approach but ultimately arguing in favour of a qualified 'propertization' of personal data).

[62] See N Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2012) (arguing that current European law can accommodate property rights in personal data and that such rights may strengthen data subjects' ability to exercise control over others' processing of data on them, particularly in an era of widespread commodification of such data).

[63] See, inter alia, Hondius (n 48) 103–5; S Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania L Rev 707, 735–6; KG Wilson, *Technologies of Control: The New Interactive Media for the Home* (University of Wisconsin Press 1988) 91–4; R Wacks, *Personal Information: Privacy and the Law* (Clarendon Press 1989) 49; Y Poullet, 'Data Protection between Property and Liberties—A Civil Law Approach' in HWK Kaspersen and

The role played by the above legal factors in catalyzing or shaping data privacy law has varied from country to country and period to period. For instance, some countries adopted data privacy statutes without having comprehensive FOI legislation already in place (for example, Germany and the UK) or without specifically recognizing a right to privacy in their legal systems (for example, Australia and the UK). Some countries failed to see the close parallels between data privacy law and FOI law when these laws were first adopted (for example, France).[64] Other countries adopted the two types of law as a single legislative package (for example, Canada and Hungary).

D. Regulatory Cross-Fertilization and Colonization

The exercise of legal influence in the data privacy field has not been simply unidirectional; data privacy law is inspiring changes in other legal fields. This cross-fertilization has come furthest in the interaction of data privacy law and human rights law. On the one hand, the emergence of data privacy law has engendered greater readiness to construe treaty provisions on the right to privacy as containing data privacy guarantees.[65] On the other, such readiness serves to stimulate the enactment or strengthening of data privacy legislation and to anchor it more firmly in traditional human rights doctrines, thereby influencing the way it is conceptualized.

In other areas, we see only the beginnings of a potential cross-fertilization process. An example is the interaction of data privacy law with competition law. In at least one jurisdiction (Belgium), elements of data privacy law have infused traditional doctrines on 'fair competition'.[66] However, the scale of

A Oskamp (eds), *Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe* (Kluwer Law & Taxation Publishers 1990) 161–81; J Litman, 'Information Privacy/Information Property' (2000) 52 Stanford L Rev 1283; Bygrave (n 35) 111.

[64] See further, H Burkert, 'Access to Information and Data Protection Considerations' in C de Terwangne, H Burkert, and Y Poullet (eds), *Towards a Legal Framework for a Diffusion Policy for Data held by the Public Sector* (Kluwer Law & Taxation Publishers 1995) 23, 49.

[65] See further Ch 2 (section I(2)).

[66] See the judgment of 15 September 1994 by the Tribunal de commerce de Bruxelles in *Aff CCH v Générale de Banque*, and the judgment of 7 July 1994 by the Tribunal de commerce d'Anvers in *Aff Feprabel et Fédération des courtiers en Assurances v Kredietbank NV*, both reported in (1994) Droit de l'informatique et des télécoms, no. 4, 45–55. The plaintiffs (two federations of insurance agents in the one case; a financial credit bureau in the other) sued two banks for engaging in unfair competition occasioned by the banks' use of a particular strategy for marketing their services at the expense of similar services offered by the plaintiffs. In both cases, the strategy in dispute involved the banks analysing data on their clients which they had acquired in the course of normal banking operations, to offer the clients certain financial services (in the one case, insurance; in the other case, mortgage

such infusion appears so far to be extremely modest. We have yet to see clear evidence of competition law rubbing off on the practice or conceptualization of data privacy law.

Cross-fertilization processes are very much at work within data privacy law itself. These concern the interaction of various countries' regulatory cultures in the field. The international codes on data privacy clearly manifest the results of such interaction. Those codes are a co-production of rules by various countries that each bring to bear their own particular tradition and perspective. As elaborated in the next chapter, this co-production has occurred across fairly broad geographical and ideological divides.

Data privacy law is also being applied in a process of regulatory colonization. By this is meant that the law is applied to an area that it was not originally conceived to cover (strong colonization) or it is used as the primary model for developing *sui generis* rules for that area (weak colonization; fertilization). The most salient area in which these processes are occurring is the regulation of biobanks containing human organic material. This is an area where, in some countries, a regulatory vacuum pertains or, in other countries, the pre-existing regulation is parlous.[67]

Denmark's data privacy regime is an example of strong colonization. The Danish DPA (Datatilsynet) has determined that human biological material contains 'personal information' insofar as the material can be linked to individual persons, and that non-electronic systematic processing of such material by private sector entities falls within the ambit of Denmark's Personal Data Act 2000.[68] The DPA has further held that a structured collection of such material (that is, a biobank) constitutes a manual (non-electronic) 'filing system' ('register') for the purposes of the Act.[69] The Agency took a similar view of the status of biobanks under Denmark's previous data protection legislation.[70]

loans) that undercut the same sorts of services already received by the clients from the plaintiffs. The plaintiffs claimed that the strategy breached the finality principle laid down in Belgian data privacy law and that this breach also resulted in violation of doctrines on fair competition. The judges found for the plaintiffs in both cases.

[67] Bygrave (n 9) 21 and references cited therein.

[68] Case 2000-321-0049 described in *Datatilsynets årsberetning 2000* [*Annual Report 2000*] (August 2001) 27–8. See further also M Hartlev, 'The Implementation of Data Protection Directive 95/46/EC in Denmark' in D Beyleveld, D Townend, S Rouillé-Mirza, and J Wright,(eds), *Implementation of the Data Protection Directive in Relation to Medical Research in Europe* (Ashgate 2004) 60, 69.

[69] Section 3(3) defines such a system as 'any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis'.

[70] See eg, P Blume, *Personregistrering* (3rd edn, Akademisk 1996) 151 regarding the Public Authorities' Registers Act 1978 (*Lov nr 294 af 8 juni 1978 om offentlig myndigheders registre*) (repealed).

As for weak colonization, we see examples of this in recent recommendations from the Council of Europe and OECD dealing with biobanks.[71] The recommendations are closely modelled on data privacy law. Their rules for use of body samples largely parallel the data privacy rules that would otherwise apply to the information generated from such samples.

E. Actors in the Field

A profusion of actors shape and apply data privacy law. Their roles may be categorized according to two main spheres of activity. One sphere concerns the operationalization of data privacy law, more specifically the ways in which the law is actually applied to specific data-processing operations or to the information systems that support these operations. I term this the 'operative sphere'. The other sphere concerns the drafting, adoption, and amendment of data privacy law. I call this the 'legislative sphere', although the term is used in a broad sense and covers some activities that are only indirectly connected to concrete legislative processes.

1. Actors in the operative sphere

In relation to the operative sphere, data privacy law typically accords at least three categories of actors with competence to decide how the law shall be applied in concrete situations. One category is the data subject—that is, the person to whom the data relates.[72] Data subjects typically exercise their decision-making competence pursuant to rules requiring their consent as a precondition for data processing, or rules permitting them to request access to data kept on them by others. Another category of actor is the data controller (hereinafter also termed simply 'controller'). This is the person or organization which determines the purposes and means of data processing. The controller need not be in possession of personal data; the crucial criterion is control. Under many laws, that control may also be shared.[73] Controllers bear chief liability for complying with the data-processing principles stipulated by the laws.

[71] Council of Europe Recommendation Rec (2006) 4 on Research on Biological Materials of Human Origin (adopted 15 March 2006); OECD Recommendation on Human Biobanks and Genetic Research Databases (adopted 22 October 2009) with accompanying guidelines.

[72] See eg, DPD Art. 2(a) which defines 'personal data' as 'any information relating to an identified or identifiable natural person ("*data subject*")' (emphasis added).

[73] See eg, DPD Art. 2(d) which defines 'controller' as the 'natural or legal person, public authority, agency or any other body which alone *or jointly with others* determines the purposes and means of the processing of personal data' (emphasis added).

A third category of actor is the DPA. The competence of DPAs tends to be more powerful than that of controllers: they usually have, for instance, the power to review (that is, to consider and overturn) the decisions of the latter.[74] They may sometimes have the power to determine the conditions for certain forms of data processing independently not just of controllers' wishes but also those of data subjects (for example, the case under a licensing regime).[75]

These actors are not the only ones with operative competence under data privacy law, yet it is they who most commonly exercise it. Courts and tribunals may also have such competence, but this will typically be exercised only on appeal from a DPA decision. In other words, the competence of the tribunal or court will typically be exercised as a power of review instigated by complaint. In many jurisdictions, this power of review tends to be exercised only exceptionally—as indicated in section A. Moreover, its 'operative' impact may be further reduced where the appeal body is limited to passing judgment on points of law rather than fact, or where the range of remedies that the body may apply is narrow.[76]

Another category of actor that figures expressly in data privacy law is the data processor (hereinafter also termed simply 'processor'). This is the person or organization which actually carries out the processing (including collection, registration, and storage) of data. For the purposes of data privacy law, processors are typically subservient to controllers—when they process personal data, they do so 'on behalf of' the latter,[77] and they act only under the latter's instructions.[78]

2. Actors in the legislative sphere

In developing and shaping data privacy law, the Council of Europe (CoE), Organisation for Economic Cooperation and Development (OECD), United Nations (UN), and EU have for a long time played the main roles at the

[74] See further Ch 6 (section A). [75] See Ch 6 (section C).

[76] The case under the US federal Privacy Act 1974. A US federal court can only issue enforcement orders relating to the exercise of persons' rights to access and rectify information relating to themselves. The court can also order relief for damages in limited situations but cannot otherwise order US federal government agencies to change their data-processing practices. See further PM Schwartz and JR Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Michie Law Publishers 1996) 100, 114ff.

[77] See DPD Art. 2(e) which denotes a 'processor' as a person or organization engaged in processing of personal data 'on behalf of' a data controller.

[78] See eg, DPD Art. 17(3): 'The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that… the processor shall act only on instructions from the controller'. Note, though, that the General Data Protection Regulation proposed by the European Commission in 2012 vests processors with greater independent responsibility than under the DPD: see further Ch 2 (section E(3)).

international level, although not always uniformly or concurrently. A large range of other inter- and non-governmental organizations have played a relatively marginal, though not insignificant, role in setting data privacy standards. These include the World Trade Organisation, International Labour Organisation, World Intellectual Property Organisation, International Telecommunications Union, and World Wide Web Consortium.[79] A particularly notable development over the last decade is the emergence of organizations in the Asia-Pacific and African regions as policy-brokers in the field. These include the Asia-Pacific Economic Cooperation (APEC) and Economic Community of West African States (ECOWAS).[80]

Beyond these organizations lies a vast array of bodies and interest groups which have pushed—and continue to push—particular privacy policies. Some are groups advocating relatively strong regimes for protection of personal data. Foremost among such bodies in the public sector are the regional groupings of national DPAs. These consist primarily of the Data Protection Working Party set up under Article 29 of the EU Data Protection Directive ('A29WP'),[81] the International Working Group on Data Protection and Telecommunications,[82] and the Asia-Pacific Privacy Authorities (APPA).[83] Of these, the A29WP has been the most influential in shaping policy with transnational impact.[84]

Flanking these are civil society groups with strong pro-privacy agendas. Prominent examples are the Electronic Privacy Information Center[85] and Privacy International.[86] These groups, though, tend to have relatively weak impact on the formulation of major international agreements.

Ranged usually against them are industry groups, such as the International Chamber of Commerce and the European Direct Marketing Association, determined to ensure that privacy safeguards do not unduly dent business interests. These groups were particularly active lobbyists during the drafting of the EU Data Protection Directive.[87] They are also heavily engaged in trying to shape the outcome of current negotiations over the proposed new EU Data Protection Regulation. Their efforts have been bolstered by the recent preparedness of major US-based software corporations, such as Facebook and

[79] For a somewhat dated, though still useful overview of these and other international players in the field, see JR Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 Stanford L Rev 1315, 1355ff. As Reidenberg makes clear, many of these bodies approach data privacy matters from a market-oriented rather than human rights perspective.

[80] The central data privacy initiatives of a selection of these organizations are presented in Ch 2.

[81] See <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>.

[82] See <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>.

[83] See <http://www.appaforum.org/>.

[84] See further Ch 6 (sections A and E).

[85] See <http://epic.org/>.

[86] See <https://www.privacyinternational.org/>.

[87] See generally Regan (n 29).

Google, to flex financial and lobbying muscle in order to thwart the introduction of more stringent data privacy legislation.[88]

Additionally, particular individuals have frequently exercised significant influence in the shaping of data privacy law and policy.[89] These are persons who, singly and together, have combined expertise in the field with strong persuasive powers and a fairly compelling vision of how law and policy ought to be developed. Examples are Alan Westin,[90] Spiros Simitis,[91] Michael Kirby,[92] Peter Hustinx,[93] and, more recently, Viviane Reding.[94] While such policy entrepreneurs have usually exercised influence under the aegis of particular organizations, they have sometimes succeeded in stamping their personal vision on the policy of the respective organization.

3. Public concern for privacy

The emergence and expansion of data privacy law reflects, at least indirectly, concern for privacy on the part of the general public. That concern, though, has rarely resulted in mass political movements with privacy protection high on their agenda. In the words of Bennett, '[t]here is no concerted worldwide privacy movement that has anything like the scale, resources or public recognition of organizations in the environmental, feminist, consumer protection, and human rights fields'.[95] A rare example of mass mobilization in the name of privacy was the public protest in Australia in 1987 over the proposal for a national identity card, the Australia Card. Yet the protest's

[88] J Guynn and M Lifsher, 'Silicon Valley uses growing clout to kill a digital privacy bill', *Los Angeles Times*, 3 May 2013, <http://articles.latimes.com/2013/may/03/business/la-fi-digital-privacy-20130503>.

[89] Bennett (n 27) 127–52.

[90] Prior to his death in 2013, Professor of Public Law and Government, Columbia University; author of several pioneering works on data privacy; founder of the think tank, Privacy & American Business.

[91] Professor of Labour and Civil Law and of Legal Informatics, Johann Wolfgang Goethe-Üniversität, Frankfurt am Main; Data Protection Commissioner for the German State of Hessen (1975–91); Chair of the Council of Europe Committee of Experts on Data Protection (1982–86).

[92] Justice of the High Court of Australia (1996–2009); President of the International Commission of Jurists (1995–98); inaugural chair of the Australian Law Reform Commission (1975–84); head of the expert group tasked with drafting the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

[93] Inaugural European Data Protection Supervisor (2004–13); President of the Dutch DPA (1991–2003); Chair of the A29WP (1996–2000).

[94] Vice President of the European Commission and in charge of the Commission's 'Justice, Fundamental Rights and Citizenship' portfolio.

[95] CJ Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press 2008) 199. See also generally Bennett (n 27) 146, 243. See too PM Regan, 'The United States' in JB Rule and G Greenleaf (eds), *Global Privacy Protection. The First Generation* (Edward Elgar 2008) 50, 71

momentum and mass rapidly diminished once the proposal was shelved.[96] Those pushing to introduce or strengthen data privacy law tend thus to be a relatively small elite.

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 nineteenth century, at least in the USA 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. As Westin observes, it was 'essentially a protest by spokesmen for patrician values against the rise of the political and cultural values of "mass society" '.[97] This would be, however, an inaccurate (and unfair) characterization 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.[98]

Those concerns seem to be broadly similar across the Western world.[99] Public opinion surveys provide abundant evidence that the levels of concern are relatively high,[100] at least in the abstract.[101] The concern for privacy is often

(observing that privacy concern amongst the US public tends to be latent rather than aggressive—'[p]rivacy appears to be one of those low level concerns that do not mobilize people to anger or action').

[96] Greenleaf (n 39).

[97] Westin (n 36) 348–9. See further JH Barton, 'Warren and Brandeis, The Right to Privacy, 4 Harv L Rev 193 (1890): Demystifying a Landmark Citation' (1979) 13 Suffolk University L Rev 875–922; DW Howe, 'Victorian Culture in America' in DW Howe (ed), *Victorian America* (University of Pennsylvania Press 1976) 3–28. For a similar critique with respect to the ideological and class roots of German 'Persönlichkeitsrecht', see P Schwerdtner, *Das Persönlichkeitsrecht in der deutschen Zivilordnung* (J Schweitzer Verlag 1977) 7, 85, 92.

[98] See too Bennett (n 27) 29.

[99] 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': see Bennett (n 27) 43.

[100] See eg, Bygrave (n 35) 110 and references cited therein; CJ Bennett and CD Raab, *The Governance of Privacy. Policy Instruments in Global Perspective* (2nd edn, MIT Press 2006) 56–65 and references cited therein. The survey material referenced there derives mainly from the USA, Canada, Australia, Norway, Denmark, and the UK. Survey material from Hungary seems largely to fit with the findings from the other countries: see I Székely, 'New Rights and Old Concerns: Information Privacy in Public Opinion and in the Press in Hungary' (1994) Informatization and the Public Sector 99–113; I Székely, 'Hungary' in JB Rule and G Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar 2008) 174, 191ff. 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 eg, WH Dutton and RG Meadow, 'A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties' in KB Levitan (ed), *Government Infostructures* (Greenwood Press 1987) 167; Regan (n 95) 71.

[101] 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 eg, Bygrave (n 35) 110, and references cited therein.

accompanied by considerable pessimism over existing levels of privacy, along with lack of trust that organizations will not misuse personal information.[102] As noted earlier, privacy concerns tend to cut across a broad range of political leanings (within liberal democratic ideology), although there are occasional indications of statistically significant variation in attitudes to privacy issues based on party-political attachments.[103] 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 from survey to survey.[104]

The survey evidence points to increasing public sensitivity to potential misuse of personal information. And we find, for example, concrete instances where items of information that previously were routinely publicized are now subject to relatively stringent requirements of confidentiality.[105] Perhaps more interesting, however, is whether indications exist of an opposite development—that is, increasing *acclimatization* of people to situations in which they are required to divulge personal information and an adjustment of what they perceive as problematic for their privacy. Such a development could lead to reductions in the stringency and scope of data privacy rules.

Prominent figures in the ICT industry have opined that privacy is now passé. The most famous case is the laconic answer given in 1999 by Scott McNealy, then head of Sun Microsystems, to a question about which privacy-enhancing measures were to be implemented in a newly launched software package: 'You already have zero privacy. Get over it'.[106] These sorts of self-serving statements are not necessarily indicative of broader public opinion. Nonetheless, it is commonly assumed that so-called 'digital natives'—those born after 1980 who are immersed in the online world—are less concerned about privacy than are those from older generations. The assumption derives

[102] Bygrave (n 15) 171, and references cited therein.

[103] H Becker, 'Bürger in der Modernen Informationsgesellschaft' in *Informationsgesellschaft oder Überwachungsstaat* (Hessendienst der Staatskanzlei 1984) 343, 415–16 (citing survey results from (West) Germany showing that supporters of the Green Party (*Die Grünen*) were more likely to view data protection as important than were supporters of the more conservative political parties).

[104] Compare eg, Székely, 'New Rights and Old Concerns' (n 100) 69 (Hungarian survey results appear to show that demographic variables play little role in determining public attitudes to privacy issues) with Office of Australian Federal Privacy Commissioner, *Community Attitudes to Privacy*, Information Paper 3 (AGPS 1995) (demographic variables play significant role in Australian survey results).

[105] See eg, H Torgersen, 'Forskning og personvern' in RD Blekeli and KS Selmer (eds), *Data og personvern* (Universitetsforlaget 1977) 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).

[106] 'Sun on Privacy: Get over It', *Wired*, 26 January 1999; available at: <http://www.wired.com/politics/law/news/1999/01/17538>.

from the apparent tendency of digital natives to disseminate a greater amount of information about themselves in online arenas than do older persons and this is also supported by some reasonably reliable evidence.[107] Yet other reliable evidence qualifies it.[108] Little solid survey evidence addressing other aspects of the 'acclimatization' issue appears to exist.[109]

F. Issues of Nomenclature and Conceptualization

The short-hand nomenclature used to describe the field of data privacy law varies considerably. The issue of nomenclature might be dismissed as trivial since it primarily relates to 'packaging'. Yet the packaging sends important signals about the law's remit, particularly to newcomers.

In the USA and many other English-speaking countries, the term 'privacy' has figured centrally in the nomenclature given to the field. This reflects the prominence accorded to privacy, both as concept and right, in these countries' discourse about the societal challenges posed by computerization. As elaborated in section C, these challenges were instrumental in stimulating the birth of data privacy law. When extensive discussion about the societal

[107] See eg, C Paine U-D Reips, S Stieger, A Joinson, and T Buchanan, 'Internet Users' Perceptions of "Privacy Concerns" and "Privacy Actions"' (2007) 65 Intl J of Human-Computer Studies 526–36 (presenting survey evidence indicating that older respondents—these came from around the world, with the largest groups coming from Russia (20 per cent) and Germany (9 per cent)—were more likely than younger respondents (ie, those under 20 years of age) to be concerned about privacy in an online context); Teknologirådet, *Holdninger til personvern* (Teknologirådet 2004) (documenting that Norwegian youths are less worried than older persons about the consequences of personal data misuse).

[108] See eg, A Lenhart and M Madden, 'Teens, Privacy, and Online Social Networks' (Pew Research Center 2007), available at: <http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx>, (presenting survey evidence indicating that many American teenagers care about their privacy and take a variety of measures to safeguard it in an online context); Paine and others (n 107) (reporting that approximately 45 per cent of respondents aged under 20 were concerned about privacy online; this figure climbed to approximately 60 per cent for respondents aged 21–30 years). Cf M Madden, A Lenhart, S Cortesi, U Gasser, M Duggan, A Smith, and M Beaton, 'Teens, Social Media, and Privacy' (Pew Research Center 2013), available at: <http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx>, (presenting survey evidence that American teenagers are sharing more information about themselves on social media sites, such as Facebook, than in the past and that the majority of them are not very concerned about third parties gaining access to the information; at the same time, most of them set their Facebook profiles to 'private').

[109] For a general review of recent survey evidence on point, see the report by the European Network of Excellence in Internet Science (EINS): S Passi and S Wyatt (eds), *Overview of Online Privacy, Reputation, Trust, and Identity Mechanisms* (EINS Consortium 2013) ch 3, available at: <www.internet-science.eu/sites/internet-science.eu/files/biblio/EINS_D5_1_1_final_0.pdf>.

implications of computerized processing of personal data first took off in the USA during the 1960s, privacy was invoked as a key term for the interests that were perceived to be threatened.[110]

The focus on privacy was far from surprising. The semantics of privacy were (and are) sufficiently broad and malleable to address what was then (and still is) seen as a fundamental danger of computer (mis)use, namely the enhanced potential for large organizations to amass data on individuals and thereby subject the latter to excessive control. The notion of privacy had already enjoyed a long, although somewhat inconsistent, tradition of use in US discourse, particularly as designating a sphere in which a person could be free of unwanted intrusion by others. This dimension of privacy is most famously summed up in the phrase 'the right to be let alone'.[111] While privacy, thus conceived, can be threatened by the intrusive activities of private sector organizations,[112] Americans have usually exercised greatest concern for it in relation to state activities.[113] The latter figured centrally in the debate that began in the 1960s over the dangers of computerization. 'Privacy' was not the only term invoked to sum up what was viewed as being at stake. A variety of other, closely related terms were invoked too, such as 'freedom', 'liberty', and 'autonomy'.[114] At the same time, the semantics of privacy were reshaped to address more directly the challenges of the computer age. Thus, the seminal literature on point conceived 'privacy' essentially as a form of information control—that 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'.[115]

The subsequent debates in other countries over the threats posed by modern ICT generally followed the lines of the earlier US discourse. As Hondius writes, '[a]lmost every issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale'.[116] The salience of the notion of privacy in US discourse helped to ensure its prominence

[110] See eg, Westin (n 36) and Miller (n 36).

[111] See esp. Warren and Brandeis (n 53) 205 (arguing that the right to privacy in Anglo-American law is part and parcel of a right 'to be let alone'). Further on the historical role of privacy in US discourse, see eg, PM Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995).

[112] Indeed, it was alleged transgressions of the boundaries of decency and the law by the 'yellow press' which provoked Warren and Brandeis to pen their article.

[113] See generally, EJ Eberle, *Dignity and Liberty: Constitutional Visions in Germany and the United States* (Praeger 2002); JQ Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale LJ 1151.

[114] As evidenced in the title of Westin's work (n 36).

[115] Westin (n 36) 7.

[116] Hondius (n 48) 6.

in debate elsewhere. This is most evident in other English-speaking countries[117] and in international forums where English is a working language.[118] Yet much of the same discourse in countries where English is not the main language has also been framed, at least initially, around notions roughly equating with privacy. Examples are 'la vie privée' (French),[119] 'die Privatsphäre' (German),[120] and 'privatlivets fred' (Danish and Norwegian).[121]

The salience of 'privacy' and closely related notions in this context ultimately reflects the Western liberal democratic heritage of the countries concerned. It is in countries with such a heritage that discourse on data privacy issues first flourished. This heritage is not the sole factor behind this chronology; the relatively advanced degree of computerization in these countries played a role as well. Yet liberalism structured the basic reactions of these countries' citizens and governments to the technological development. It is an ideology that traditionally accords the privacy of individuals a great deal of value.[122] Liberal democratic states typically embrace what Bennett and Raab term the 'privacy paradigm'. This is a set of assumptions which idealizes civil society as made up of 'relatively autonomous individuals who need a modicum of privacy in order to be able to fulfil the various roles of the citizen in a liberal democratic state'.[123] This paradigm sensitizes the citizens and governments concerned to the privacy-related threats posed by ICT.

Nevertheless, the regulatory field which crystallized from the early European discussions on point is often described using a bland, technocratic

[117] For the UK, see eg, Committee on Privacy (the Younger Committee), *Report of the Committee on Privacy*, Cmnd 5012 (HMSO 1972) and P Sieghart, *Privacy and Computers* (Latimer 1976); for Canada, see eg, Department of Communications and Department of Justice, *Privacy and Computers: A Report of a Task Force* (Information Canada 1972); for Australia, see eg, Australian Law Reform Commission (ALRC), *Privacy*, Report no. 22 (AGPS 1983) and WL Morison, *Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General*, Report no. 170/1973 (AGPS 1973).

[118] See eg, Council of Europe (CoE) Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (adopted 26 September1973); CoE Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector (adopted 24 September 1974).

[119] See eg, G Messadie, *La fin de la vie privée* (Calmann-Levy 1974).

[120] See eg, the 1970 proposal by a (West) German Interparliamentary Working Committee for a 'Gesetz zum Schutz der Privatsphäre gegen Missbrauch von Datenbankinformationen': described in H-P Bull, *Datenschutz oder Die Angst vor dem Computer* (Piper 1984) 85.

[121] See eg, Denmark's Register Committee (Registerudvalget), *Delbetænkning om private registre*, Report no. 687 (Statens trykningskontor, 1973).

[122] See eg, S Lukes, *Individualism* (Blackwell 1973) 62; O Mallmann, *Zielfunktionen des Datenschutzes: Schutz der Privatsphäre, korrekte Information. Mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen* (A Metzner 1977) 17.

[123] Bennett and Raab (n 100) 4.

nomenclature avoiding explicit reference to 'privacy' or closely related terms. This nomenclature is 'data protection', derived from the German term 'Datenschutz'.[124] The nomenclature has gained broad popularity in Europe and it is occasionally used elsewhere.[125] While 'privacy' and 'data protection' are closely linked, Europeans often stress that the two are not identical, reserving 'data protection' for a set of norms that serve a broader range of interests than simply privacy protection.[126]

A third term for the field is 'data privacy'. The term has entered the discourse more recently than 'privacy' and 'data protection'. It is gaining traction on both sides of the Atlantic.[127] Its use can be seen as an attempt to signal more accurately than the other two terms the focus, thrust, and rationale of the relevant norms.

Additionally, we find various countries and regions displaying terminological idiosyncrasies that partly reflect different jurisprudential backgrounds for the discussions concerned. In Western Europe, the discussion has often drawn upon jurisprudence developed there on legal protection of personality. Thus, 'Persönlichkeitsrecht' and 'Persönlichkeitsschutz' figure centrally in German and Swiss discourse on data privacy.[128] Norwegian discourse revolves around the notion of 'personvern' ('protection of person(ality)'),[129] while Swedish discourse focuses on 'integritetsskydd' ('protection of (personal) integrity').[130] By contrast, South American discourse often revolves around the notion of 'habeas data' (roughly meaning 'you should have the data'). This derives from due-process doctrine based on the writ of habeas corpus.[131] To take yet another example, US discourse (in addition to focusing

[124] Further on the origins of 'Datenschutz', see Simitis (n 24) 78–9.

[125] See eg, GL Hughes and M Jackson, *Hughes on Data Protection in Australia* (2nd edn, Law Book Company 2001).

[126] See eg, EDPS (n 35) 15, 21.

[127] As evidenced by the title of this book and the title of the journal, *International Data Privacy Law*, published by OUP from 2011. See too eg, Schwartz and Reidenberg (n 76); C Kuner, *European Data Privacy Law and Online Business* (OUP 2003).

[128] See eg, Germany's Federal Data Protection Act 1990 (*Bundesdatenschutzgesetz—Gesetz zum Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990*) § 1(1) (stipulating the purpose of the Act as protection of the individual from interference with their 'personality right' ('Persönlichkeitsrecht')); Switzerland's Federal Data Protection Act 1992 (*Loi fédérale du 19. juin 1992 sur la protection des données/Bundesgesetz vom 19. Juni 1992 über den Datenschutz*) Art. 1 (stating the object of the Act as, inter alia, 'protection of personality' ('Schutz der Persönlichkeit')).

[129] See Bygrave (n 35) 138–43 and references cited therein.

[130] See eg, Sweden's Personal Data Act 1998 (*Personuppgiftslagen*, SFS 1998:204) s 1; Bygrave (n 35) 126–9 and references cited therein.

[131] Habeas data is a personal right of action provided for in the constitutions of a number of Latin American countries. It may be invoked before a constitutional court to require an organization to disclose data it holds on the plaintiff, to correct inaccuracies in the data, and in some cases to destroy the data. It is said to be inspired by the CoE Convention on data protection (described in Ch 2,

on 'privacy', 'freedom', and 'autonomy') employs the notion of 'fairness' to describe core data privacy principles, referring to these as principles of 'fair information practice'.[132]

All up, the field shows bewildering conceptual and terminological diversity. This hampers easy comprehension of its remit. Adding to this difficulty is the polysemantic, diffuse character of many of the above-mentioned concepts. The most famous case in point is 'privacy'. Various definitions of the concept abound. A lengthy debate has raged, predominantly in US circles, about which definition is most correct.[133] We find parallel debates in other countries which centre on similar concepts,[134] although these debates appear less extensive than the privacy debate. Some of the latter debate concerns whether privacy is best characterized as a state/condition, a claim, or a right. That issue aside, the debate reveals four principal ways of defining privacy.[135] One set of definitions is in terms of *non-interference*,[136] another in terms of *limited accessibility*.[137] A third set conceives of privacy as *information control*.[138] A fourth set incorporates various elements of the other three sets but links privacy exclusively to *intimate* or *sensitive* aspects of persons' lives.[139]

section B) and the 1983 Census Act decision of the German Federal Constitutional Court (described in Ch 6 (n 45)). See A Guadamuz, 'Habeas Data: The Latin-American Response to Data Protection' (2000) JILT, no. 2, available at: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/>; A Guadamuz, 'Habeas Data vs the European Data Protection Directive' (2001) JILT, no. 3, available at: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz>. See also Ch 3 (section C). However, it is worth noting that Westin mentioned the possibility of developing such a writ already at the beginning of the 1970s: see AF Westin, 'Civil Liberties and Computerized Data Systems' in M Greenberger (ed), *Computers, Communications, and the Public Interest* (The Johns Hopkins Press 1971) 151, 168. The writ has also gained traction in South-East Asia and Africa. In January 2008, the Supreme Court of the Philippines formally adopted a 'Rule on the Writ of Habeas Data' (AM No. 08-1-16-SC; in force 2 February 2008) as a Rule of Court. And provision for habeas data is made in Art. 46 of the Cape Verdean Constitution (last revised 2010) and Art. 69 of the 2010 Angolan Constitution.

[132] See eg, DHEW (n 31) 41; US Privacy Protection Study Commission, *Personal Privacy in an Information Society* (US Government Printing Office 1977) esp. 17, 21.

[133] For useful overviews, see D Solove, *Understanding Privacy* (Harvard University Press 2008) chs 1–2; JC Inness, *Privacy, Intimacy, and Isolation* (OUP 1992) ch 2; JW DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press 1997) chs 2–3.

[134] See eg, *En ny datalag* (SOU 1993:10) 150–61 (documenting difficulties experienced in Swedish data protection discourse with respect to arriving at a precise definition of 'personlig integritet').

[135] Bygrave (n 35) 128–9.

[136] See eg, Warren and Brandeis (n 53).

[137] See eg, R Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale LJ 421, 428–36 (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')).

[138] See eg, Westin (n 36) 7.

[139] See eg, Inness (n 133) 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').

Definitions of privacy in terms of information control tend to be most popular in discourse dealing directly with law and policy on data privacy.[140] Indeed, the notion of information control has arisen as a leitmotif for this discourse, both in Europe and the USA. 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' (for example, in the case of Swedish discourse),[141] or it stands alone. The most significant instance of the latter is the German notion of 'informational self-determination' ('informationelle Selbstbestimmung') which in itself forms the content of a constitutional right first recognized in a landmark decision of the Federal Constitutional Court (Bundesverfassungsgericht) in 1983.[142]

In this light, it is obviously very difficult if not impossible to come up with one concise formulation that accurately depicts the remit of the field. By 'concise' is meant a phrase consisting of two or three words. The term 'data protection' is problematic on multiple counts. It fails to indicate expressly the central interests served by the norms to which it is meant to apply. It is misleading insofar as it 'suggests that *the data* are being protected, instead of *the individual* whose data are involved'.[143] It has an 'unnecessary technical and esoteric air'.[144] And it has connoted in some circles concern for data security[145] and for protection of intellectual property rights.[146] It is claimed to have an advantage over a 'privacy'-focused nomenclature as it 'distinguishes the policy problem that has arisen since the late 1960s from the broad social value that has such a rich tradition and important place in the liberal democratic heritage'.[147] Yet this line-drawing capability can also underplay lines of continuity in the types of interests protected.

A term such as 'privacy protection' or 'privacy law' faces problems also. One difficulty is that 'privacy' suffers from a heritage of definitional instability and imprecision. Another is that the term fails to capture the entire remit of the law concerned. As shown in section A, this failure is a case of both

[140] See generally Bygrave (n 35) 130 and references cited therein.

[141] See eg *En ny datalag* (n 134) 159 (noting that the concept of 'personlig integritet' embraces information control).

[142] Decision of 15 December 15 1983, BVerfGE (*Entscheidungen des Bundesverfassungsgerichts*) vol 65, 1. See further Ch 6 (n 45).

[143] ACM Nugter, *Transborder Flow of Personal Data within the EC* (Kluwer Law & Taxation Publishers 1989) 3.

[144] Bennett (n 27) 76.

[145] See n 5 and accompanying references.

[146] Schwartz and Reidenberg (n 76) 5 (observing that the notion of data protection in the USA often 'evokes intellectual property principles of copyright and trade secrets as well as technological security measures').

[147] Bennett (n 27) 14.

under-inclusion and over-inclusion. It is a case of under-inclusion in that data privacy law embraces more than what are typically regarded as privacy concerns.[148] It is a case of over-inclusion in that 'privacy' as such has various dimensions (spatial, bodily, etc.) with which data privacy tends not to deal directly.[149]

What of a nomeclature built up around the notion of 'fairness', such as 'fair information practises law'? At first sight, this sort of terminology is attractive given that the agenda of data privacy law can be summed up quite well in terms of concern for ensuring fairness in the processing of personal data.[150] Yet 'fairness' is somewhat nebulous and has a variety of connotations, some of which have little relevance to the concerns of data privacy law.[151] Another problem is that the terminology could be applied equally well to describe, say, copyright legislation; in other words, the terminology on its own does not single out what is unique for the law concerned. Much the same criticisms can be made of a nomenclature based on the notion of 'secrecy',[152] or of attempts to subsume data privacy law under the parole of 'rule of law' or related notions, such as 'Rechtssicherheit' and 'rettssikkerhet'.[153]

My choice to employ 'data privacy' as the primary label for this area of law is not because I judge it as perfect. The label shares the problems of under-inclusion and definitional instability identified with a 'privacy'-focused nomenclature. However, it reduces the latter's over-inclusion problem. Moreover, it communicates relatively well—and far better than 'data protection'—one of the central interests at stake. It also provides a bridge for synthesizing European and non-European legal discourses.

[148] See further, Bygrave (n 35) ch 7.

[149] Further on those dimensions and their interaction with data privacy law, see Bygrave (n 9) 1–7.

[150] Bygrave (n 35) 155–6.

[151] Eg, the keeping of promises and bargains (quid pro quo obligations)—a dimension of 'fairness' that is central in J Rawls, *A Theory of Justice* (OUP 1972) esp. sections 18 and 52.

[152] See Inness (n 133) 60–1 (arguing that data privacy law ought to be characterized as protecting secrecy rather than privacy). An additional flaw with such a characterization is that data privacy law is about far more than just ensuring non-disclosure of information.

[153] For related criticism of the latter possibility, see eg, DW Schartum, *Rettssikkerhet og systemutvikling i offentlig forvaltning* (Universitetsforlaget 1993) 72, 85ff. Cf S Eskeland, *Fangerett* (2nd edn, TANO 1989) 79 (placing data privacy interests under the umbrella of 'rettssikkerhet'); LJ Blanck, 'Personvern—nytt navn på "gamle" rettsspørsmål?' (1979) Lov og Rett 117, 122–3 (taking a similar approach to Eskeland).