Lee A. Bygrave

43 Privacy and data protection

Abstract: This entry elucidates the semantics of privacy and data protection, taking account of transnational variations in how they are understood. Their interrelationship is also explained as is their relationship to closely linked concepts, such as data security and bio-privacy. Finally, the entry briefly canvasses legal and social norms for safeguarding privacy and personal data.

Keywords: privacy, data protection, data security, secrecy, surveillance, law

Introduction

Privacy is a term about which there has been a long and ultimately unresolved debate concerning its proper meaning. Literature devoted to its semantics is massive (for useful overviews, see DeCew, 1997; Solove, 2008; Koops et al., 2017). Much of the literature is philosophical and legal but contains significant input from other disciplines. These include sociology, psychology, and criminology, along with their more specialized offshoots, such as surveillance studies. The debate over the semantics of privacy escalated during the 1980s and 1990s, largely in conjunction with discussion over the societal effects of increasing mass surveillance (see Surveillance by Lyon)—i. e., the systematic monitoring of ever greater numbers of persons and ever larger amounts of personal data with a view to exercising control or generating profit (see, e. g., Flaherty, 1989; Lyon and Zuriek, 1996; Lyon, 2007; Zuboff, 2019). Privacy has been flagged as a key interest (or congeries of interests) that is seriously threatened by such development, particularly in the context of crime control and surveillance capitalism. Yet, somewhat paradoxically, arriving at a precise, universally agreed definition of privacy has proven well-nigh impossible. This is partly because of the nebulous, loose, and somewhat haphazard way in which the term is often used, and partly because it is multifaceted—as elaborated below.

The semantics of data protection have also come to the fore in conjunction with discussion concerning mass surveillance. Like privacy, data protection is typically pitched as an important bulwark for upholding civil liberties in the face of state and business interests in exploiting personal data for various ends—national security, crime control, organizational efficiency, profit generation, etc. However, the semantics of data protection are far easier to navigate than those pertaining to privacy. Broad consensus exists as to the core meaning of data protection, and the legal-regulatory context in which it is applied is significantly more bounded than is the case for privacy. Whereas privacy denotes an interest (or set of interests) that potentially range(s) across all existential contexts, data protection denotes a set of norms and other regulatory measures pertaining to the processing of a particular type of data. Nonetheless, use of the term presents challenges. For persons who are unfamiliar with it, data protec-

 https://doi.org/10.1515/9783111062037-044

tion on its face may be easily conflated with data security and similar security-specific terms such as computer security and cybersecurity, yet, as shown below, data protection is not fully commensurate with security of data. Further, the term is anemic in the sense that it fails to flag the interests and values served by the norms and measures it denotes. This has led to considerable debate over the rationale of data protection as a regulatory endeavor (see, e.g., Bygrave, 2002; Bygrave, 2025). Part of that debate is the nature of the connection between privacy and data protection—in particular, the degree to which data protection is predominantly concerned with safeguarding privacy.

Privacy semantics in greater depth

Defining privacy is a challenging and contentious endeavor. Adding to the challenge is that many non-English languages do not operate with direct counterparts of 'privacy.' For instance, a commonly used equivalent for privacy in Chinese is 'yinsi,' which connotes a shameful secret (Lü, 2005). However, privacy is not the same as secret, which may be defined in terms of "intentional concealment" (Bok, 1982: 5), nor is privacy necessarily shameful. To take another example, the closest equivalents to privacy in Norwegian are 'privatlivet' ('private life') and 'privatlivets fred' (the peace of private life): neither term is fully commensurate with all the various possible connotations of privacy, as shown below. Thus, persons who do not have English as their native language may struggle to get a complete sense of privacy's many facets.

A related challenge springs from the ideological underpinnings of privacy-focused discourse, which is most extensively developed in Western cultures with strong liberalist traditions. As Lukes observes, 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" (Lukes, 1973: 62). The fact that much of the discourse on privacy as a threatened interest tends to assume the virtue of Western liberalist assumptions undercuts its global appeal. Nonetheless, there are also 'privacy skeptics' within the Western sphere who question the societal desirability of robust privacy protections —e.g., from economic, communitarian, or feminist viewpoints (see, e.g., Posner, 1978; Etzioni, 1999; Allen, 1988).

A recent comprehensive mapping of privacy's dimensions across various fields, including law, parses privacy into eight basic types (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioral), with a ninth type (informational) as an overlapping but distinct overlay to the former types (Koops et al., 2017). The study is not intended to be exhaustive but underscores the huge semantic and contextual space that privacy occupies.

Sometimes, particular aspects of this space are specifically flagged by adding a prefix to 'privacy.' An example is 'bio-privacy,' which is used to denote the "privacy issues of biometric technology" (Liu, 2012: 21), thus emphasizing the bodily, behavioral, and informational dimensions. Bio-privacy concerns become relevant primarily in respect of the deployment of biometrics-based systems of identification or verification/authen-

tication—for instance, iris-scanning devices for controlling access to closed-off spaces as part of border/immigration control, or automated facial recognition cameras for identifying criminal suspects in crowds (see Biometric Failure by Magnet and Din). Another, closely related example is 'genetic privacy,' which is typically used to denote protection from non-voluntary disclosure of genetic information (see, e.g., Allen, 1997; Lunshof et al., 2008).

At the same time, it is important to note how new technologies and organizational practices are blurring or merging the various dimensions of privacy. A salient instance is the gradual ontological evisceration of the traditional distinction between the physical/physiological human body as such and information about the body, brought on by the increased focus on the body as a source of information, particularly due to developments in genetic testing and biometrics. In this respect, van der Ploeg refers to an emergent "ontology of informatized bodies" (van der Ploeg, 2005). There is growing legal recognition of this trend, exemplified in the willingness of courts and legislators to treat human biological material, such as DNA (deoxyribonucleic acid), as personal data subject to data protection norms (see DNA/Big Genome Data by Kaufmann). The 2008 judgment of the European Court of Human Rights in *S and Marper v. United Kingdom* is a case in point, with the Court stating that cellular samples from persons who were apprehended by the police constitute personal data for the purposes of the Council of Europe Convention on Data Protection (see further Bygrave, 2010: 7–8).

Scholarly conceptions of privacy frequently have differing focal points in respect of the term's radius. One conception pitches privacy predominantly in terms of non-interference. The most famous example in point is Warren and Brandeis' definition of the right to privacy in US law as the "right to be let alone" (Warren and Brandeis, 1890). Another conception pitches privacy as a state of limited accessibility (e.g., Gavison, 1980; Bygrave, 2002). A third conception of privacy is as a claim to information control. Westin's definition of privacy is a landmark instance of this view: "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" (Westin, 1970: 7). A fourth conception connects privacy exclusively to intimate or sensitive facets of persons' lives. Upon this view, disclosure of non-intimate or non-sensitive information about a person does not diminish their privacy (e.g., Inness, 1992; Wacks, 1989). Yet another conception brings context to the fore. A key instance is Nissenbaum's framing of privacy in terms of 'contextual integrity,' whereby privacy is essentially concerned with maintaining respect for the structure of social settings (Nissenbaum, 2010). In this perspective, privacy speaks to the preservation of formal and informal social norms as to what behaviour (e.g., regarding information disclosure) is appropriate in particular spheres of life or activity. For instance, privacy would uphold the reasonable expectation that the norms for information disclosure in bedroom activity differ significantly from the norms for information disclosure in publicly accessible places.

The aforementioned list of conceptions is not exhaustive but is sufficient to convey the variation of perspectives on privacy's semantic core. From the list, it becomes evident that there are also differences over whether privacy in itself is best understood as

a state of being or as a normative position, such as a moral claim or legal right, and over whether privacy is a form of autonomy or a completely independent category of state or interest.

The semantics of data protection in greater depth

The term 'data protection' derives from the German term 'Datenschutz.' The latter has roots in terminology denoting security of data (namely, 'Datensicherung' and 'Datensicherheit'). However, data protection and its German equivalent were coined in order to flag a set of measures and concerns that go well beyond simply ensuring data security (Simitis, 2006: 62–63).

Data protection denotes a set of measures specifically aimed at regulating the processing of data relating to, and facilitating identification of, persons (i.e., personal data) in order to safeguard, at least partly, the privacy and related interests of those persons. The measures embody a set of largely procedural principles addressing, *inter alia*, the purposes of the data processing and the quality of the data, and stipulating measures to ensure that the processing is transparent to, and capable of being influenced by, the person to whom the data relate ('data subject'). In most countries, these principles and measures have been set into legislation, and the resultant corpus of law tends accordingly to be termed 'data protection law.' The EU's General Data Protection Regulation (GDPR) of 2016 is a landmark example in point.

However, the nomenclature for this sort of law is not uniformly termed 'data protection.' In certain countries outside Europe, such as the US, Australia, Canada, and New Zealand, this body of law tends to be labeled 'privacy law,' 'information privacy law' or, more recently, 'data privacy law.' This labeling reflects in part the central place of 'privacy' in these countries' public debates over the societal implications of computerized processing of personal data (see Data Justice by Redden). For instance, when these debates first took off in the US during the 1960s, privacy was invoked as a key term for the interests that were perceived to be threatened (Westin, 1970). At the same time, the semantics of privacy were (and remain) sufficiently broad and flexible to address what was then (and still is) regarded as a basic danger of computer (mis)use, namely the increased potential for large organizations to amass data on individuals and thereby subject them to excessive control (Bygrave, 2002, 2025). Even in Europe, the right to respect for private life is frequently construed and applied as a weapon of data protection, also by the EU Court of Justice and the European Court of Human Rights (Bygrave, 2025). Further, the notion of 'informational self-determination' has become a leitmotif for much of data protection law, and this notion fits comfortably with Westin's conception of privacy as a form of information control (Westin, 1970). Thus, there are close ties between privacy and data protection.

Nonetheless, it bears emphasis that data protection and privacy are not fully commensurate with each other. Data protection law embraces more than what are typically regarded as privacy concerns (Bygrave, 2025). And, as elaborated above, privacy as such

has various dimensions (spatial, bodily, etc.) with which data protection tends not to deal directly.

Similarly, data protection is not fully commensurate with data security. Although data security is a component of data protection, the latter embraces other rules and measures too. Moreover, data security on its own may serve a broader range of concerns than data protection: whereas a central aim of data protection is safeguarding data subjects' privacy-related interests, data security as such can also be aimed at safeguarding the interests of users of all kinds of data (not just personal data) in the name of, say, national security. The same applies with the overlapping areas of information security, information systems security, and cybersecurity. The security measures are mainly directed towards ensuring that data are processed in line 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, and availability of information in an information system as well as appropriate protection of the system itself, wherein 'confidentiality' indicates that the information and system are protected from unauthorized disclosure, 'integrity' describes their protection from unauthorized modification, and 'availability' denotes that they are accessible and usable on demand by authorized actors, systems, or programs (Bygrave, 2021). In many cases, these measures may serve to promote data protection, but they can obviously come into conflict with the latter as well.

Implementation of privacy and data protection measures

Protection of privacy and personal data is achieved through a variety of means. Public attention tends to be directed towards high-profile legislative measures, such as the GDPR, which constitutes, in the eyes of many, the most globally influential 'gold standard' of its kind (Bradford, 2020). This perception is partly due to the GDPR's relatively powerful sanctions and enforcement regime. However, the strength of that regime has proven to be significantly greater 'on paper' than in practice (see, e. g., Gentile and Lynskey, 2022), thus underlining (yet again) that the classic gap between 'law in books' and 'law in practice' tends to be extremely difficult to bridge. Concomitantly, the level of privacy and data protection 'on the ground' tends only to be partly a function of legislative or judicial efforts; other measures often play an equally or more significant role. These include soft law instruments in the form of technical standards, recommendations, codes of practice, and the like. Yet, arguably, the most enduring constituents of the societal bedrock of privacy and data protection are more informal or intangible behavioural norms rooted in context-sensitive notions of social propriety.

Conclusions

- Although signifying important determinants of the quality of societal life, both privacy and data protection remain contested, nebulous concepts.
- The semantics of privacy are especially difficult to comprehend due to the disparate ways in which the term tends to be invoked and the multiplicity of its dimensions.
- Nonetheless, claims that privacy and data protection are too vacuous to be analytically or normatively useful should be rejected; although they both suffer from terminological imprecision, they each have a sufficiently tangible core of meaning to warrant their continued use in legal-regulatory policy and other public discourse.

Suggested reading

Bygrave, L. A. (2025). *Data Privacy Law: An International Perspective.* 2nd ed. Oxford: Oxford University Press.

Koops, B.-J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, 38, 483 – 575.

Solove, D. (2008). *Understanding Privacy.* Cambridge, MA: Harvard University Press.

References

Allen, A. (1988). *Uneasy Access: Privacy for Women in a Free Society.* Totowa, NJ: Rowman & Littlefield.

Allen, A. (1997). Genetic privacy: Emerging concepts and values. In M. A. Rothstein (ed.), *Protecting Privacy and Confidentiality in the Genetic Era* (pp. 31 – 59). New Haven: Yale University Press.

Bok, S. (1982). *Secrets: On the Ethics of Concealment and Revelation.* New York: Pantheon.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World.* Oxford: Oxford University Press.

Bygrave, L. A. (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits.* The Hague: Kluwer Law International.

Bygrave, L. A. (2010). The body as data? Biobank regulation via the 'back door' of data protection law. *Law, Innovation and Technology*, 2, 1 – 25.

Bygrave, L. A. (2021). Security by design: Aspirations and realities in a regulatory context. *Oslo Law Review*, 8(3), 126 – 177.

Bygrave, L. A. (2025). *Data Privacy Law: An International Perspective.* 2nd ed. Oxford: Oxford University Press.

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology.* Ithaca, NY: Cornell University Press.

Etzioni, A. (1999). *The Limits of Privacy.* New York: Basic Books.

Flaherty, D. H. (1989). *Protecting Privacy in Surveillance Societies.* Chapel Hill, NC: University of North Carolina Press.

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal*, 89, 421 – 471.

Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *International & Comparative Law Quarterly*, 71(4), 799 – 830.

Inness, J. C. (1992). *Privacy, Intimacy, and Isolation.* Oxford: Oxford University Press.
Koops, B.-J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, 38, 483 – 575.
Liu, N. Y. (2012). *Bio-Privacy: Privacy Regulations and the Challenges of Biometrics.* London: Routledge.
Lü, Y.-H. (2005). Privacy and data privacy issues in contemporary China. *Ethics and Information Technology*, 7, 7 – 15.
Lukes, S. (1973). *Individualism.* Oxford: Blackwell.
Lunshof, J., Chadwick, R., Vorhaus, D., & Church, G. M. (2008). From genetic privacy to open consent. *Nature Reviews Genetics*, 9, 406 – 411.
Lyon, D. (2007). *Surveillance Studies: An Overview.* Cambridge: Polity Press.
Lyon, D., & Zuriek, E. (1996). *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press.
Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Redwood City, CA: Stanford University Press.
Posner, R. A. (1978). The right to privacy. *Georgia Law Review*, 12, 393 – 422.
Simitis, S. (ed.) (2006). *Bundesdatenschutzgesetz.* 6th ed. Baden-Baden: Nomos Verlagsgesellschaft.
Solove, D. (2008). *Understanding Privacy.* Cambridge, MA: Harvard University Press.
van der Ploeg, I. (2005). *The Machine-Readable Body: Essays on Biometrics and the Informatization of the Body.* Maastricht: Shaker Press.
Wacks, R. (1989.) *Personal Information: Privacy and the Law.* Oxford: Clarendon Press.
Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4, 193 – 220.
Westin, A. F. (1970). *Privacy and Freedom.* New York: Atheneum.
Zuboff, S. (2019). *The Age of Surveillance Capitalism.* London: Profile Books.