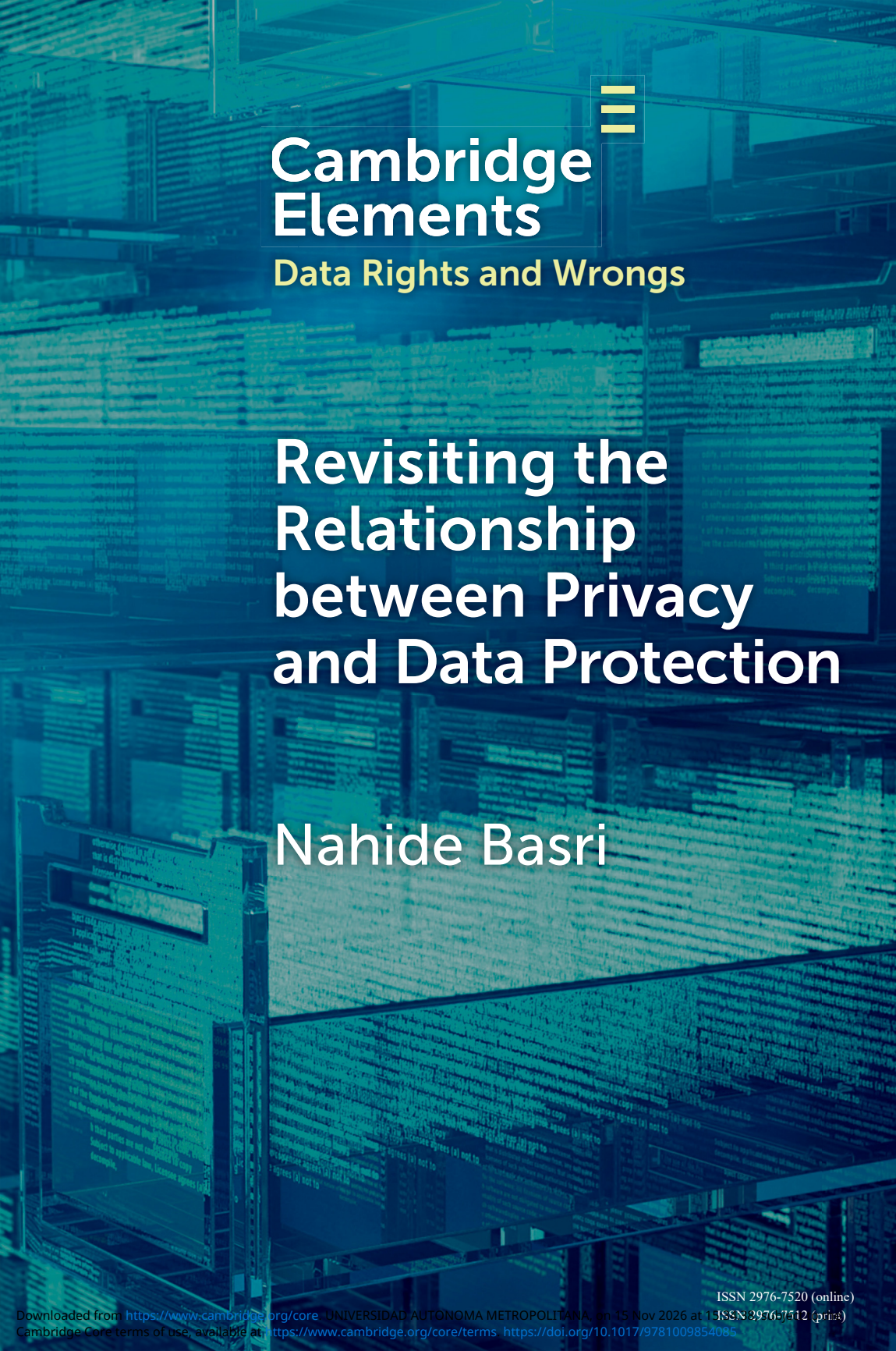


ISSN 2976-7520 (online)
ISSN 2976-7512 (print)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:58:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Cambridge Elements

Elements in Data Rights and Wrongs
edited by
Damian Clifford
London School of Economics
Jeannie Marie Paterson
University of Melbourne

REVISITING THE RELATIONSHIP BETWEEN PRIVACY AND DATA PROTECTION

Nahide Basri
UCL Laws

CAMBRIDGE UNIVERSITY PRESS

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085



Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781009854078
DOI: 10.1017/9781009854085

© Nahide Basri 2026

This publication is in copyright. Subject to statutory exception and to the
provisions of relevant collective licensing agreements, with the exception of the
Creative Commons version the link for which is provided below, no reproduction
of any part may take place without the written permission of Cambridge University
Press & Assessment.

An online version of this work is published at doi.org/10.1017/9781009854085
under a Creative Commons Open Access license CC-BY-NC-ND 4.0 which
permits re-use, distribution and reproduction in any medium for non-commercial
purposes providing appropriate credit to the original work is given. You may not
distribute derivative works without permission. To view a copy of this license,
visit https://creativecommons.org/licenses/by-nc-nd/4.0

When citing this work, please include a reference to the DOI 10.1017/9781009854085

First published 2026

A catalogue record for this publication is available from the British Library

*A Cataloging-in-Publication data record for this Element is available from the
Library of Congress*

ISBN 978-1-009-85407-8 Hardback
ISBN 978-1-009-85409-2 Paperback
ISSN 2976-7520 (online)
ISSN 2976-7512 (print)

Cambridge University Press & Assessment has no responsibility for the persistence
or accuracy of URLs for external or third-party internet websites referred to in this
publication and does not guarantee that any content on such websites is, or will
remain, accurate or appropriate.

For EU product safety concerns, contact us at Calle de José Abascal, 56, 1°, 28003
Madrid, Spain, or email eugpsr@cambridge.org.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the
Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Revisiting the Relationship between Privacy and Data Protection

Elements in Data Rights and Wrongs

DOI: 10.1017/9781009854085
First published online: July 2026

Nahide Basri
UCL Laws

Author for correspondence: Nahide Basri, nahide.basri.22@ucl.ac.uk

Abstract: This Element revisits the unsettled relationship between (information) privacy and data protection, exploring why it remains elusive, complex, and often misunderstood. It does so by integrating conceptual, regulatory, and legal analysis. First, it identifies and discusses three conceptualisations of privacy in the literature, arguing that they should be understood complementarily rather than alternatively to provide a layered account of privacy. Second, it examines how each of these conceptualisations is reflected in the language and substance of key regional and international data protection frameworks. Third, it analyses their relationship through a legal lens, assessing the extent to which core data protection principles appear in human rights jurisprudence on the right to privacy. By bringing together these strands of analysis, it demonstrates that privacy and data protection overlap yet remain non-identical, and illustrates why their boundaries remain difficult to delineate. This title is also available as Open Access on Cambridge Core.

Keywords: data protection, privacy, the right to privacy, human rights, information privacy

© Nahide Basri 2026

ISBNs: 9781009854078 (HB), 9781009854092 (PB), 9781009854085 (OC)
ISSNs: 2976-7520 (online), 2976-7512 (print)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Contents

Introduction 1

1 (Information) Privacy 2

2 Data Protection: Emergence and Development of the Core Principles, Relationship to (Information) Privacy 18

3 The Relationship between the Right to Privacy and the Core Data Protection Principles under Human Rights Law 44

4 Conclusion 69

Appendix 71

References 72

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Introduction

The relationship between privacy and data protection remains conceptually unsettled. Beyond a broad agreement in the literature that the two are closely connected, their relationship has been framed in different and often conflicting ways: data protection has variously been described as, inter alia, a subset to, flipside, companion, continuation of or an autonomous right distinct from privacy (e.g. Rouvroy, 2008; De Hert and Gutwirth, 2009; Tzanou, 2013; Lynskey, 2014). This conceptual confusion is both reflected in and compounded by the main regional and international data protection frameworks. Early international frameworks – i.e. the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by the Organisation for Economic Co-operation and Development (OECD), Convention 108 for the Protection of Individuals with regard to Processing of Personal Data by the Council of Europe (CoE), and the United Nations Guidelines concerning Computerised Personal Data Files – treat data protection either as equivalent to the right to privacy or as a tool primarily aimed at safeguarding that right. Differently, at the European level, the adoption of the Charter of Fundamental Rights (CFR) has provided for separate rights to privacy and data protection, but without really articulating the rationale for introducing data protection as a distinct right (Lynskey, 2014). Expressly inspired by the EU and also reflecting the constitutional traditions of its Member States, the Standards for Personal Data in the Ibero-American States (Ibero-American Standards) similarly articulate two separate 'fundamental' rights, although this is of rhetorical rather than legal effect given these Standards' non-binding status. Conversely, other regional frameworks such as the Organisation of American States (OAS) Principles on Privacy and Personal Data Protection and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework seemingly treat privacy and data protection interchangeably, albeit not always so clearly or consistently. This variation in how different data protection frameworks articulate or implicate their relationship to privacy is particularly perplexing since, as this Element demonstrates, they establish substantively similar core data protection principles. The jurisprudence on the right to privacy under human rights law further muddles this landscape. By incorporating most, but not all, core data protection principles, this jurisprudence points to an intricate relationship between privacy and data protection that extends beyond mere intersection. Yet, this jurisprudence often lacks the depth, consistency, and conceptual clarity needed to elucidate this relationship.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

This Element revisits the long-standing debate on this relationship, with a view to exploring why it remains so elusive, confused, and often misunderstood. In doing so, it also seeks to develop a more nuanced understanding of both privacy and data protection. Section 2 begins by examining three dominant conceptualisations of (information) privacy that can be identified in the literature and categorises them as separation-based, control-based, and power-based perspectives. Although often presented as alternatives, each of these perspectives captures important facets of privacy. Importantly, they overlap in some respects and address one another's limitations in others, and should therefore be considered together to offer a layered understanding of privacy. Section 3 turns to data protection, outlining the objectives underpinning key international and regional frameworks and the core principles they share. It then explores how the privacy conceptualisations from Section 2 resonate within these instruments, revealing the multilayered relationship between privacy and data protection, neither of which can be understood in singular terms. Finally, Section 4 tests these findings under human rights law by comparing the protections offered under data protection frameworks with those developed in privacy jurisprudence. Bringing together the conceptual, regulatory, and legal analyses, this Element argues that privacy and data protection are heavily overlapping yet non-identical, while also showing why the non-overlapping areas are so difficult to delineate. It concludes by discussing the implications of the existing ambiguities in the current state of literature, law, and practice.

1 (Information) Privacy

The primary challenge in defining the relationship between privacy and data protection lies in the inherent difficulty of conceptualising privacy itself. Indeed, although the ubiquitous use of 'privacy' in daily language gives the impression of an obvious and widely shared meaning, such consensus is contingent on a high level of abstraction (Inness, 1996: 3). Attempts to define and concretise privacy resemble navigating 'an unknown swamp', with the 'ground soften[ing]' as one uncovers the confusion and disparity 'underlying our privacy intuitions' (Inness, 1996: 3).

The law and literature refer to privacy at times as a state of seclusion and withdrawal and, at other times, as one's ability to control others' access to oneself. Some accounts of privacy focus instead on its normative value, connecting it with, inter alia, autonomy (Roessler, 2018), self-identity (Hildebrandt, 2015), intimacy (Fried, 1968; Gerstein, 1978; Inness, 1996; Schoeman, 1984), personhood (Benn, 1984; Reiman, 1976), dignity

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

and integrity (Bloustein, 1964; Moreham, 2008), anti-totalitarianism (Rubenfeld, 1989), political freedom (Richards, 2013; Rubenfeld, 1989: 737), or freedom more widely (Roessler, 2018). The resulting landscape has been often characterised as a state of 'morass' (Nissenbaum, 2010), 'chaos' (Inness, 1996), and 'disarray' (Solove, 2008: 39). Part of the perplexity arises from the fluid nature of the right to privacy, which has broadened over time to respond to a multitude of emerging social concerns, ultimately encompassing 'a range of wildly disparate interests' (BeVier, 1995: 458). Its scope has extended, for instance, from a right to abortion (in light of the growing respect for women's sexual/reproductive autonomy) to one's interest in protecting their personal information (in response to challenges posed by new technologies). Such multifariousness complicates efforts to identify a common thread across the different interests that have fallen within its umbrella.

This Element does not purport to offer a totalising account of privacy. Rather, it recognises the multidimensional nature of privacy and focuses on information privacy as a specific facet thereof, given its particular relevance to – and complex relationship with – data protection. What information privacy encompasses is precisely the subject of this section, but broadly, it refers to one's interest in how their information is processed (e.g. collected or used) by others. Other dimensions of privacy in the existing taxonomies include decisional privacy (interest in exercising one's agency without external undue influence); bodily and spatial privacy (interest in controlling others' access to, respectively, one's body and private spaces such as one's home); intellectual privacy (interest in developing opinions and beliefs without others' interference; Richards, 2008: 389); communicational privacy (interest in controlling others' access to one's communications); and attentional privacy (interest in freedom from the attention of others). Notably, these dimensions overlap and have been framed differently by different commentators (e.g. O'Hara, 2023; Koops et al., 2017: 483). The focus on information privacy in this Element is therefore neither absolute nor exclusive; other dimensions of privacy – and privacy more broadly – are also drawn on where relevant.

This section explores information privacy by examining the three main ways in which the scholarship has conceptualised it. It sets out and critically examines the two mainstream perspectives – 'separation'-based and 'control'-based accounts (see, e.g., Inness, 1996) – before turning to power-based perspectives, which emerged as critiques of the former. Importantly, delineating these accounts is an exercise in approximation, aiming to capture the main ways of thinking about information privacy rather than

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

offering sharply defined categories. Indeed, it is not always possible or easy to identify which authors adhere to which conceptualisation, and, at times, the same author may be understood differently depending on how or which aspects of their work are read or emphasised. At the same time, the differences that do exist between the three perspectives do not always challenge, but sometimes complement, one another. Specifically, separation-based accounts adopt a scopic approach, focusing on delimiting the boundaries of information privacy. Differently, control-based accounts take a functional perspective, focusing not on what constitutes information privacy but on how it should be protected. Power-based critiques highlight the limitations of both approaches in responding to power asymmetries generated and exacerbated by modern technologies, while also complementing them by drawing attention to broader information-processing structures.

While all three perspectives on information privacy contain both descriptive elements (what information privacy *is*) and normative elements (what information privacy *protects*), power-based perspectives operate at a different level compared with the other two accounts. They function more as a *critique* than as a standalone *account* of what information privacy (descriptively) is. Their focus lies in highlighting the *normative* connection between privacy and power; any descriptive observations they offer tend to emerge indirectly (and more fragmentarily) through their critique of the descriptive assumptions of the two mainstream accounts. Furthermore, power-based critiques – mainly adopted in jurisdictions such as the US – often focus not on privacy per se but on privacy *laws* (by which they often refer to data protection *laws/frameworks*, as examined in Section 2). This blurs the distinction between privacy as an *interest* and privacy as a *legal* right/protection, while *also* conflating privacy and data protection. The interchangeable use of 'privacy' and 'data protection' also reflects particular terminological choices in certain jurisdictions, which further complicates and obscures the privacy-data protection relationship (as revisited below). This section explores each conceptualisation of information privacy in turn, demonstrating how they differ from, but also complement, one another. To be clear, the following discussion focuses on privacy as an interest rather than on its legal protection, the latter being discussed in Section 3.

1.1 Separation-Based Accounts: Privacy as Concealment of the 'Private Realm'

Separation-based accounts of information privacy stem from traditional understandings of privacy as a broader, multidimensional concept. The

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

literature on the latter can accordingly be usefully drawn on here, although it does not specifically address information privacy, which gained prominence more recently with new technologies. These traditional accounts conceptualise privacy as the protection of an individual's private realm from intrusion by others. This understanding can be traced back to the work of Warren and Brandeis – the first articulators of the *right* to privacy – who described it as 'the "right to be let alone"' (Warren and Brandeis, 1890: 195; for further information on the origins of privacy, see Richardson, 2017). Even though the authors frame privacy as a 'right', their work seems to propose an account of privacy (which they argue had to be protected by a legal right that was missing at the time). Their account frames privacy as the existence of boundaries between one's inner life – 'the sacred precincts of private and domestic life' – and 'the [outside] world' (Warren and Brandeis, 1890: 195–196). Interestingly, although this account conceptualises privacy broadly, it was rooted in concerns about unprecedented intrusions into individuals' domestic lives *enabled by emerging technologies of the time*, specifically '[i]nstantaneous photographs and newspaper enterprise' which made information about individuals' private lives available on an unprecedented scale. This closely echoes the concerns at the heart of information privacy accounts more specifically.

In informational terms, the private sphere guarded under these accounts corresponds to the so-called private information. This can be understood either as information that is inherently private (e.g. relating to individuals' personal, sensitive, or intimate matters, such as their health or sexual life) or as information that is not inherently private but can only be obtained 'by eavesdropping, spying, or other means generally considered intrusive' (see, e.g., Nissenbaum, 1997: 213). This understanding brings two categories of information within the scope of information privacy: information private *by content* (*per* its sensitive/intimate/personal nature) or information private *by context* (*per* how it is obtained, e.g., through intrusion into private zones).[1] The latter – private information by context – underscores the inextricable connection between informational and other dimensions of privacy, whereby the intrusion upon the latter (e.g. entry into one's home, a space protected by spatial privacy) also defines the scope of intrusion upon the former (extending, e.g., to seemingly mundane/non-sensitive information obtained from that protected

[1] Although not all 'separatist' scholars adopt this twofold understanding of private information: e.g. Gerety suggests that privacy pertains to information concerning the 'intimacies of personal identity', thereby excluding private information by context (Gerety, 1977: 72).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

space, such as, say, the floor plan of one's home). By emphasising the (restrictive) scope of what falls within privacy, these accounts advance a conception of information privacy – applicable equally to information privacy as one of its dimensions – characterised by three underlying features: first, that privacy entails a state of seclusion, measured through inaccessibility vis-à-vis others; second, that privacy is a negative concept, understood as non-intrusion; and third, that privacy functions to shelter the individual – and perhaps their close social circle such as friends/family, as discussed below – from 'others'.

Separation-based accounts highlight that protecting the 'private realm' is essential to securing identity, autonomy, freedom, and dignity, yet they often leave unexplained the assumptions linking these values – both to one another and to privacy itself. Unpacking these links requires drawing on insights from various scholars. Hildebrandt provides a helpful starting point, arguing that privacy provides a negative freedom from 'unlawful [i.e. unjustified] interference' of the others (2015: 80). This negative freedom provides a 'safe cocoon to hide in', which then enables positive freedom to 'build and rebuild identity beyond the continuous pressures of social stereotyping, public opinion, and dominant frames of reference' (Hildebrandt, 2015: 80), thereby supporting a sphere of decisional privacy. The causal link between these interests can be framed as follows: privacy creates a space for freedom and autonomy, enabling individuals to develop identity and personhood, thereby fostering individuality. It also safeguards dignity, as its denial – through perpetual transparency and the unwanted gaze – can reduce individuals to objects of observation rather than autonomous agents. The power asymmetries this generates between the watcher and watched overlap with the power-based critique, further developed below. Separation-based and power-based perspectives also converge in another important respect: while the former are primarily defined in individualist terms, they nonetheless accommodate privacy's broader importance in fostering democracy, societal well-being, creativity, and political freedom, as well as in serving as a bulwark against totalitarianism, as also emphasised by the power-based perspectives (Richards, 2022: 134; Hughes, 2015).

Accordingly, separation-based accounts offer important insights into the role and value of a key aspect of privacy: the interest in being secluded from others. In informational terms, this pertains to the restriction of 'private information' from others. Indeed, the main critique of these accounts lies not in their claims but in their omissions. This Element focuses on two interlinked aspects of information privacy that separation-based accounts

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

may not fully capture. First, the public–private dichotomy that lies at the heart of separation-based accounts tends to exclude privacy interests in public spheres. By extension, this would also exclude so-called public information, namely, information that is not inherently private by nature *and* which is available in the public domain (i.e. outside private spheres) (see also González Fuster, 2014: 22). Yet this public–private dichotomy is no longer justifiable. It is no longer enough to protect individuals only against intrusion into their private sphere because emerging technologies mean that privacy can now *also* be undermined through public channels (Nissenbaum, 1998: 593). Indeed, individuals could once rely on attentional privacy in public spheres: they could merge into the crowd and preserve their anonymity, going about largely unnoticed. Even where noticed by some, 'any single observer' could only 'observe and harbour discrete bits of information' that would also be temporally 'limited by what any single human brain could reasonably and efficiently hold' (Nissenbaum, 1998: 576). Surveillance infrastructures now continuously monitor and record activity in both physical and virtual public spaces, as a result of which information that existed in a specific context and timeframe is no longer confined to those boundaries. Contexts and spaces are blurred, along with temporal distinctions. The record of the past is no longer necessarily sustained by 'mere human memory'; instead, technologies render the past available for 'almost instant replay' (Allen, 2011: 166). Information is collected, aggregated, and combined from various contexts and times, producing the 'mosaic effect', whereby disparate pieces of public information can be assembled to provide a comprehensive insight into a person's private realm, thereby undermining the very values privacy is meant to protect (Nissenbaum, 1998: 589; Véliz, 2024). This illustrates the fragility of the public–private distinction and suggests that a comprehensive account of information privacy must adequately account for privacy interests in the public domain, including in 'public information'.

The second limitation of separation-based accounts is that, by focusing on the division between the self (the private) and the rest (the public), they risk advancing an overly individualistic view of privacy and, ultimately, of human nature (Inness, 1996: 43–44). This overlooks the fact that privacy and the interests it protects, such as individuality, are shaped by and dependent on one's surroundings, relationships, and interactions (Goffman, 1959: 253). Privacy may include – but cannot be 'reduced to' – 'a fixed condition' such as utter seclusion; it is better understood as a dynamic process that enables an individual to set and manage their boundaries vis-à-vis others (Cohen, 2012: 1906; Nippert-Eng, 2010: 25;

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Solove, 2007: 763; Richardson, 2017: 122); this also highlights the role of privacy in facilitating social interaction (Hughes, 2012). Admittedly, the recognition that privacy can also be social and relational – although largely advanced by those adhering to control-based accounts – is not incompatible with separation-based accounts. The latter can accommodate this aspect by framing the protected private sphere as encompassing not only the individual but also their close relationships and social circles, provided that sharing of information remains confined to that sphere (e.g. Warren and Brandeis, 1890; Richardson, 2017:122). To that extent, separation-based accounts may overlap with control-based accounts, albeit to a limited extent: the overlap ceases once information enters the public sphere, at which point separation-based accounts would suggest that the (information) privacy interest is extinguished. Differently, control-based accounts *can* treat the same act – sharing information with the public – as an *exercise* of information privacy (see Section 1.2). The main limitation of separation-based accounts, then, lies in their emphasis on 'separation', which either overlooks or only narrowly acknowledges the significance of individuals' interactions with one another in the exercise of their privacy.

Ultimately, separation-based accounts capture an important *aspect* of privacy, including of information privacy – the restriction of private information from others – which enables and fosters values such as personhood, individualism, and resistance to totalitarianism. The emphasis on the inaccessibility of private information, however, does not sufficiently account for privacy interests in 'public' information and individuals' relationships in the public sphere outside one's 'private life'. Indeed, these criticisms hold only if the separation-based accounts are understood as presenting information privacy in comprehensive and exclusivist terms – which this Element argues against, as it now turns to other perspectives on information privacy.

1.2 Control-Based Accounts: (Information) Privacy as 'Boundary Management'

Unlike most separation-based accounts, control-based accounts more explicitly – and often, exclusively – focus on information privacy. They gained prominence in the late 1960s, particularly in response to the rise of computerised data processing technologies. Perhaps the best-known formulation of this account is Westin's definition, which, though intended to apply to privacy generally, frames it strictly in informational terms, as 'the claim of individuals, groups or institutions to determine

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

for themselves when, how, and to what extent information about them is communicated to others' (1967: 7). Control-based accounts shift the emphasis towards whether the subject has exercised control over the flow of information, adopting a functional approach. The emphasis in these accounts on (individual) control has received a 'staggering' 'consensus' (Schwartz, 1990: 820): it has dominated theorisations of not only information privacy but also privacy more generally (see, e.g., Fried, 1968: 482; Miller, 1971: 25; Gross, 1971: 71; Altman, 1975; Roessler, 2018). Notably, this understanding of information privacy is often adopted by scholars – those based in the US, Australia, and Canada – who also use the term interchangeably with data protection, given the central role of control in the latter (see Section 1.3 on jurisdictional terminology choices and Section 2.3 on the role of individual control in data protection frameworks) (Bygrave, 2010: 170; Clifford, 2024: 208). It is also worth noting here that, in line with its dominant framing within the information privacy literature, control-based accounts discussed here conceive of control in an *individualised* sense, rather than at a broader/architectural level. The latter dimension of control has emerged separately through power-based critiques of privacy (below) and within conceptualisations of data protection (Section 2.2).

Control-based accounts articulate information privacy as a 'means' for the individual to 'achiev[e] a preference about whether their data is processed', 'placing … [them] … at the center of decision-making' (O'Hara, 2023: 6; Schwartz, 1999: 820). Two elements are integral to these accounts. The first is the subjective 'preference' of the individual regarding the flow of their information. The second element is objective, concerning whether the individual is in fact able to 'achieve' their preferences. The combination of both elements distinguishes control-based accounts from separation-based accounts. The latter's exclusive focus on withholding information means that any act of making it accessible beyond the private realm is seen as the 'voluntar[y] relinquish[ment] … of … privacy' (Parent, 1983: 273; Allen, 2000: 868; Schoeman, 1984: 1–3). Conversely, the subjective element within the control-based accounts means that these accounts can characterise the same act of disclosure as the manifestation of information privacy where it aligns with the individual's subjective preferences. This means that under control-based accounts, information privacy does not end each time information is made accessible; instead, it is the ongoing capacity to exercise control over one's information and thus extends spatially and temporally as information flows across different contexts and throughout the life cycle of information processing.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

From a normative perspective, like separation-based accounts, control-based accounts frequently articulate the value of privacy (including information privacy) as self-development, personhood, dignity, and individuality. The underlying narrative that links privacy to these values is broadly shared across both accounts and is therefore not repeated here. This is with two notable differences. The first pertains to the role of autonomy. While separation-based accounts suggest that privacy carves out a space that *enables* the exercise of autonomy, control-based accounts – to the extent that they require active engagement by individuals – assume the *pre-existence* of autonomy in the exercise of privacy, which is critiqued shortly below. The second difference lies in control-based accounts' capacity to accommodate information privacy more explicitly and comprehensively. Framed as the individual's ability to manage their 'borders' vis-à-vis others, these accounts often focus on the diverse relationships that privacy helps establish and sustain. Fried, for instance, highlights the indispensability of privacy for the 'relations of the most fundamental sort: respect, love, friendship and trust' because it enables sharing information which 'one does not share with all' (1968: 484). Likewise, Gerstein argues privacy enables intimate relationships through the 'exclusive sharing' of information that 'no one else knows' about (1978: 76, 79). Although these scholars arguably fall within control-based accounts by framing privacy as control over information, their view of privacy as the exclusive sharing of information within an intimate zone shows notable overlaps with separation-based accounts. Other control-based accounts, however, move beyond this overlap by emphasising the role of privacy-as-control in enabling and sustaining a broader range of relationships, extending beyond intimate ones. For instance, Rachels suggests that the 'ability to control … who knows what about us' is preconditional to the 'ability to create and maintain different sorts of social relationships with different people' (1975: 326). Lynskey argues that this control facilitates the presentation of different facets of one's persona in different contexts, allowing one to simultaneously assume diverse roles, say, as colleagues, friends, and strangers (Goffman, 1959; Lynskey, 2015b: 218–221), although Lynskey makes these observations regarding data protection, which already hints at areas of overlap between data protection and privacy, as examined under Section 2.3. It is worth noting here that some control-based accounts – particularly those that connect (informational) privacy with intimacy – understand the scope of information covered thereunder more narrowly as one's ability to share their 'private information' (e.g. information about one's intimate lives) with others (e.g. Gerstein, 1978: 76; Parent, 1983: 70). In doing so, they

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

internalise the scopic limitations of separation-based accounts critiqued above. Yet most other control-based accounts do not specify the scope of protected information and instead refer more broadly to information about oneself (which can be broader than 'private information' as defined above, including non-sensitive information about someone in publicly available domains) (e.g. Westin, 1967).

Control-based perspectives usefully complement separation-based models by providing a functional account of *how* privacy can be exercised. However, these accounts encounter important limitations vis-à-vis modern technologies for two key reasons. First, the core assumption underpinning control-based accounts – that individuals are autonomous, informed, and capable of exercising control over their data – does not hold in power-asymmetric contexts involving modern technologies. These technologies are often deployed by powerful public or private actors with whom individuals have hierarchical, power-asymmetric relationships, undermining their ability to make informed and voluntary decisions about their information. First, much information collection occurs covertly (Solove, 2001: 1450). Purported efforts to inform people about the collection and uses of their information through the so-called privacy policies are often illusory. People typically fail to 'notice, read, or understand' these policies due to their ubiquity, resulting user fatigue, and limited time (Solove, 2013: 1885). The so-called transparency paradox compounds this problem: broad descriptions of data processing fail to enable meaningful decisions, while detailed/technical explanations often exceed the average person's ability to understand complex technologies (Richards and King, 2013: 42). Modern technologies such as data analytics may be applied to large datasets at incredible speeds to identify correlations and unprecedented inferences, meaning that previously insignificant information can acquire new meanings and significance subsequently (van der Sloot, 2020). Consequently, individuals cannot be provided with intelligible and comprehensive information about when, how, and by whom their data are processed, which is a necessary precondition for meaningful exercise of control. Structural factors further undermine individuals' decision-making. While scholars invoke the 'privacy paradox' to explain the gap between people's stated concern for privacy and their actions that fail to safeguard it (e.g. Solove, 2021), the issue arguably lies less in irrationality than in individuals' often rational sense of powerlessness and lack of agency, driven by structural power asymmetries. The cognitive burden of estimating the future value of safeguarding privacy against the immediate benefits of accessing online resources further compounds this challenge (Cohen, 2000: 1371).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Although control over information extends beyond initial consent to the entire data life cycle, structural and informational burdens undermine individuals' ability to control their information post-collection.

Second, by focusing on individuals' ability to control the flow of information, control-based accounts overlook the fact that information itself is often shared and relational, especially in light of emerging technologies (Solove, 2022: 984). To illustrate this, consider the example presented by Viljoen (2021). Adam, a former gang member, shares images of his tattoos on TattooID, an online platform for tattoo enthusiasts, whilst explicitly indicating his affiliation with this gang. Subsequently, the FBI scans the database and apprehends Ben, who possesses a similar tattoo, as a suspected gang member. This captures the relational logic of data analytics at its core: they analyse multiple (often large) datasets, identify correlations (here, a recurring connection between being a gang member and having this tattoo), and accordingly draw inferences (namely, that Ben, possessing the same tattoo, is also likely to be a gang member). The analytical process involves the 'deindividualization of the person' because it assesses and perceives people based on the collective characteristics of their respective groups rather than their individual traits and merits (Vedder, 1999: 75). Indeed, as Viljoen claims, 'it does not matter *who* the data "came" from, but *what* such data says about Ben, and *how* such meaning is used to act upon Ben' (2021: 608).

Individualised control-based accounts of information privacy encounter particular challenges here because it is difficult to qualify the *act of extrapolating* insights and inferences itself as an information privacy issue. The extrapolation seeks to generate 'knowledge about the world', pertaining to a fact or a pattern that is 'out there'. In this instance, relevant privacy issues relate rather to the FBI's access to the initial information on Adam's tattoo and gang membership, which was shared voluntarily *by Adam*, but from which the inference *about Ben* was extrapolated. The extrapolated information is used to uncover information about Ben that he has never disclosed or in whose creation/discovery he has had no control. At the same time, this extrapolation exacerbates the impact on Ben's privacy in the sense that it allows him to be targeted and profiled in more invasive ways later. The knowledge obtained renders capturing information about Ben's tattoo more meaningful, revealing more information about him. What this example illustrates, for the purposes of this section, is that genuine individual control over information can often be an illusory possibility in the modern technological landscape and thus is not a fully effective standalone tool for managing

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

information boundaries. Although individual control remains an important – if not sufficient – element, its limitations indicate that an adequate conceptualisation of information privacy cannot remain focused exclusively on privacy breaches at the individual level but must also account for the broader infrastructures of information processing. This broader focus on the informational ecosystem is reflected in power-based perspectives on information privacy, explored now.

1.3 Power-Based Perspectives: Critiquing and Complementing the Mainstream Accounts

Finally, power-based perspectives developed most recently have been gaining prominence in the literature (e.g. Solove, 2025; Richards, 2022; Véliz, 2020; Cohen, 2019a; Austin, 2014). These perspectives have emerged directly in response to the limitations of the former accounts vis-à-vis power asymmetries generated by emerging technologies. Thus, power-based perspectives both challenge some of the premises of the former two accounts and complement them by injecting further elements, elaborating in particular on the means and methods (the causes), implications (the consequences), and ways of preventing (the remedies) information privacy breaches. While often framed as alternative and self-standing accounts, this section demonstrates that they are better conceptualised as *critiques* of, or *perspectives* on, information privacy. Indeed, it also illustrates that by shifting the emphasis to power as a means of both identifying and responding to the limitations of existing conceptualisations of privacy, power-based perspectives also extend beyond privacy as such, blurring into and cascading across *other* rights and interests that information privacy breaches may undermine downstream.

Power-based perspectives focus on the complex relationship between privacy, power, and knowledge, placing surveillance – namely, the 'focused, systematic and routine attention to personal details for the purpose of influence, management, protection or direction' (Lyon, 2007: 14) – at their centre. As Cohen suggests, surveillance has both 'passive' and 'active' dimensions (2008). Passive surveillance involves receiving, collecting, and/or recording information. This is aptly captured in Foucault's theorisation of Bentham's work on the Panopticon (1991), which, although originally developed as a model of State power rather than privacy per se, now often stands at the centre of contemporary perspectives that frame privacy in power-based terms. The Panopticon imagines a circular prison architecture where the central watchman has a comprehensive view of the prisoners ('pan' meaning 'all' and 'optikon'

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

meaning 'seeing'). The design achieves the efficient enforcement of discipline, not (only) through prisoners' visibility but more fundamentally through their *perception* of being observed. The *possibility* of being seen generates a chilling effect on their behaviour. Passive surveillance often leads to and combines with active surveillance. Unlike passive surveillance, which involves recording pre-existing information, active surveillance refers to the *use* of the collected information (e.g. classifying and sorting information) to construct new inferences or imaginaries by placing people into categories. Emerging technologies, such as data analytics, facilitate this process, with their 'core and unavoidable' mode of operation being the classification and profiling of individuals based on patterns and correlations, from which inferences and predictions are drawn (see further Mittelstadt, 2017: 477).

The overarching *problematique* at the heart of power-based perspectives is the arbitrary authority that both components of surveillance confer on the surveilling party, which creates a sense of disempowerment for individuals and limits their control over how their information is used and the potential effects it may have. This concern overlaps with control-based accounts but adds distinct dimensions to it (and to separation-based accounts). Namely, while passive surveillance's chilling effect is discussed in both mainstream accounts, power-based perspectives introduce a crucial shift in focus: they highlight that the chilling effect arises not from an *actual* invasion of informational boundaries, but from the *perception* that such boundaries do not exist to begin with – regardless of the objective reality. This highlights that privacy harms can occur without a violator – which is 'precisely' why '[t]he Panopticon works' – 'because people can be mistaken about whether someone is watching them and nonetheless suffer similar or identical effects' (Calo, 2011: 1147). Similarly, the (power-based) critiques of active surveillance distinctively focus on the *unpredictability* of how information about individuals may be used against them, particularly by highlighting the mosaic effect where seemingly trivial data can (co-)produce highly sensitive insights. This challenges or complements separation- and control-based accounts, which define the scope of (informational) privacy either very narrowly or not at all. Yet, in doing so, power-based perspectives create new uncertainties about when a piece of information falls outside information privacy and often risk cascading into a general regulatory framework that conflates privacy and data protection (see also Section 3.1).

In addition to the mosaic effect, power-based perspectives highlight how the insights or inferences obtained can subsequently underpin significant

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

decisions affecting individuals, adding another layer of power over them. Zuboff, for instance, explains that such inferences predict human behaviour to target individuals with personalised services, steering them into desired patterns of action (2019). This not only channels individuals towards consuming certain products in the commercial realm, as part of the 'surveillance capitalism' project, but also extends into the political realm, interfering with democratic processes, as illustrated by the Cambridge Analytica scandal (Zuboff, 2019). Importantly, power-based perspectives stress that the impact of these practices is not limited to the individual but also extends to the creation of new realities and categories that fundamentally reshape societies in ways envisioned by those deploying the technologies. Predictive analytics exemplify this: the collection and structuring of information for these systems is never neutral but is carried out by powerful actors according to their own objectives and visions, inevitably reflecting a particular reading of the past (Gandy, 2016: 63). Gandy highlights, for instance, how racial proxies are built into these systems 'even where their inclusion made little sense at all', resulting in discriminatory and biased decision-making under the guise of scientific neutrality (Gandy, 2016). These technologies enable powerful actors not only to 'see' but also 'shape' and 'control' the future (Matsumi and Solove, 2024: 36).

Central to these concerns is the creation of a 'Kafkaesque world of bureaucracy', in which information is not only beyond the individual's control but also subjected to a bureaucratic process that is itself inadequately controlled (Solove, 2004: 96). Yet, unlike the individualised focus of control-based accounts, power-based perspectives do not treat information privacy breaches as (merely) fragmented individual harms but as systemic issues embedded in the very architectures of information processing. By placing their emphasis on power, these accounts shift the focus away from the *wrong* suffered at the individual level to the *wrongdoer* at the structural level (Austin, 2014: 160–177). Accordingly, their concern is not limited to personal loss of control but extends to the arbitrary and unchecked power embedded in the social and legal frameworks governing information processing, demonstrating that these may be harmful per se even where power is not actively exercised (Austin, 2014: 166; van der Sloot, 2017). By foregrounding the broader asymmetries within which information processing operates, power-based views suggest that the remedy does not lie – or at least does not *solely* lie – in enhancing individual control. Instead, they call for structural and institutional 'rules' aimed at 'controlling power' to avoid situations where

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

no one is meaningfully accountable for the use of personal information (Richards, 2022: 38; Austin, 2014: 100; Solove, 2001: 1428; Cohen, 2019b: 2). The remedy envisaged by power-based accounts is therefore still control, but of a different kind: control not exercised (solely) by individuals but embedded within broader structures that safeguard individuals. This conception goes beyond, albeit overlaps with, the individual-focused, control-based accounts discussed earlier. It understands control more broadly – as the creation of an environment in which individual autonomy is both supported and enabled through oversight by responsible entities (see also Cohen, 2019b: 2; Solove, 2004).

This broader notion of (architectural) control closely overlaps with conceptualisations of data protection as a system of checks and balances on information structures, as further explored in Section 2.3. There is thus a significant overlap – and a blurred boundary – between power-based perspectives on information privacy and data protection. Part of the reason for this close connection lies in jurisdictional differences in terminology and conventions, particularly between the US and the EU. Strikingly, many scholars who adopt power-based perspectives on information privacy – primarily based in the US – appear, in their accounts of privacy, to be discussing privacy *law* more broadly. By this, they often seem to be referring to what would, in the EU context, be understood as *data protection* laws and frameworks (e.g. Richards, 2022; Matsumi and Solove, 2024; Kaminski, 2022; Bennett, 1992: 14). This suggests that, in many instances, when power-based perspectives address information privacy, they are in fact engaging with data protection in a broader sense. Indeed, some of the central premises of these predominantly US-based power-based perspectives – such as the argument that privacy extends beyond individual control – often stem from what these scholars understand to be an (arguably overemphasised, as demonstrated in Section 2) focus in data protection law on individual control (see a similar observation in Clifford, 2024: 192).

Accordingly, while power-based perspectives offer valuable insights that enrich conceptualisations of information privacy – for example, by highlighting the limitations of framing information privacy solely in terms of restriction or control of information flows in the context of emerging technologies – they often extend beyond information privacy per se. This is evident in the seemingly unbounded nature of the 'information' these perspectives encompass, as well as in the range of concerns they raise regarding practices such as pervasive (active and passive) surveillance, which implicate related but distinct rights, including protection

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

from discrimination. To be sure, the latter are inextricably linked to information privacy, since their materialisation hinges on extensive collection and unforeseeable uses of individuals' information without respect for informational boundaries. But those interests seem to relate more to the *consequences* of information privacy breaches for other rights and interests than to the conceptualisation of information privacy itself. This point is acknowledged by scholars such as Zuboff, who argues that new technologies generate unprecedented challenges for which the tendency has been to rely on familiar concepts such as privacy, while admitting that those concepts 'fall short in identifying and contesting the most crucial and unprecedented facts of this new [reality]' (2019: 14). This raises broader questions about the utility of attempts to subsume all informational harms under the umbrella of information privacy, as power-based perspectives sometimes appear to do. The concern that privacy, as a familiar and well-established interest, is being stretched to accommodate novel challenges posed by emerging technologies is also at the heart of jurisprudence on the right to privacy, as explored under Section 3.

1.4 Interim Conclusions

The foregoing discussion shows that, despite their differences, separation-, control-, and power-based perspectives are complementary rather than competing. Developed at different points in time – in the order discussed – these accounts reflect evolving ways of thinking about information privacy, which do not replace but rather build on one another to form a layered understanding. Separation-based accounts stress the protection of private information as a means of safeguarding autonomy, identity, and democracy but tend to overlook privacy interests in public and relational contexts. Control-based accounts address some of these gaps by emphasising individual agency over information flows; however, they presuppose an autonomous individual capable of managing their data – an assumption that falters in power-asymmetric contexts – and they often overlook the relational nature of modern 'knowledge' production. Power-based perspectives respond to these shortcomings by examining structural disempowerment and the systemic regulation of information flows. Yet, as these perspectives frequently advance their critiques in relation to privacy laws – by which they often refer to data protection laws – their claims extend beyond information privacy to encompass other rights and interests affected by unfair processing structures. This also reflects differences in terminological choices across jurisdictions, which further contribute to confusion in the relationship between privacy and data protection.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

2 Data Protection: Emergence and Development of the Core Principles, Relationship to (Information) Privacy

Understanding the multifaceted nature of information privacy is essential for developing a more nuanced account of its relationship with data protection. As this section demonstrates, the different perspectives on information privacy – coupled with a selective focus on different aspects and dimensions of data protection – are the main reasons underlying the conceptual ambiguity surrounding the relationship between the two. To map the complex relationship between the two, this section first zooms into data protection. Section 2.1 examines the genealogy of the main regional and international data protection frameworks to bring out the concerns and objectives underpinning their origins and development, with a particular focus on whether, and if so how, they refer to privacy (which they seemingly use as a shorthand for information privacy – an approach this section follows by using 'privacy' to denote 'information privacy' thereafter for consistency and simplicity). Section 2.2 then examines the substance of these main data protection frameworks with a view to identifying the shared – what this Element calls the 'core' – principles therein, concretising what data protection encompasses in substance. Building on that analysis, Section 2.3 then critically revisits the ways in which the relationship between privacy and data protection has been framed in the literature.

It is worth specifying at the outset the precise subjects of comparison when assessing this relationship. More specifically, this pertains to clarifying the reference to data protection – which can refer either to data protection *frameworks* or to the *right* to data protection. As mentioned earlier, some data protection frameworks – especially the GDPR and the Ibero-American Standards (and several national data protection laws, whose examination falls outside this Element's scope) – articulate a right to data protection as a distinct *right* alongside the right to privacy. The introduction of such a separate right – together with the fact that this approach is not consistently adopted across other frameworks and laws – has been a principal catalyst for the debate (and resulting confusion) concerning the relationship between data protection and privacy. To complicate matters further, where the right to data protection has been established, its conceptual foundations (i.e. what this right is or what it does) have remained unclear, both within the relevant frameworks and in the corresponding literature (Clifford, 2024). These data protection frameworks articulate the right to data protection as a main, though

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

not exclusive, right protected within them. This suggests a potential gap between what the right itself protects and what the frameworks as a whole protect. Yet ambiguities surrounding the conceptual foundations of the right make it unclear which elements of data protection frameworks can properly be understood as instruments for protecting that right. As a result, the literature on the relationship between data protection and privacy often refers to data protection as composed of principles enshrined in data protection *frameworks* – even when explicitly distinguishing between the right and the framework – without fully acknowledging the limitations inherent in comparing a right (privacy) with a framework (data protection), which operate on different analytical planes. This Element likewise compares privacy with data protection frameworks, but does so with these limitations in mind. This choice is made for two reasons. First, most of the regional and international data protection frameworks examined do not articulate a distinct right to data protection. Second, where such a right is recognised, its scope, rationale, and conceptual foundations remain uncertain, making it difficult to use it as a stable basis for comparison. The question of the right to data protection is revisited in Section 2.2 (to highlight its uncertain foundations and its relationship to data protection principles) and in Section 2.3 (to examine whether data protection frameworks provide protections beyond pre-existing rights, a point further developed following the legal analysis in Section 3.3).

2.1 The Emergence of Data Protection Frameworks and Their Articulation of Their Relationship to Privacy

A brief account of the genealogy of data protection is essential for understanding how these frameworks have interpreted privacy and how this understanding has shaped their articulation of the relationship to it (see also Bosua et al., 2025). Its roots can be traced back to governments' growing need for citizen data to manage post–Second World War welfare states, which triggered in citizens a sense of loss over their personal information (González Fuster, 2014; Mayer-Schönberger, 1997). Early data protection laws accordingly started emerging in the 1970s at the national level in order to 'tame' technology and forestall the emergence of unchecked information processing bureaucracies (Mayer-Schönberger, 1997: 223). These national frameworks had a 'primarily "protective" approach', which meant that their substance was predominantly composed of ex ante obligations imposed on information processors, with limited rights afforded to individuals (Ausloos and Dewitte, 2018: 4). They accordingly tended to omit vocabulary such as 'privacy' or

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

'protection of intimate affairs', using instead 'technical jargon' such as 'data', 'data bank', and 'data file' (Mayer-Schönberger, 1997: 224; cf. the 1978 French law, which granted stronger control rights to individuals; González Fuster, 2014: 64). This anti-totalitarian origin of early data protection frameworks, oriented around checking state power, reflects an early emphasis on controlling large-scale information processing. This mirrors the power-based perspectives on (information) privacy, which however only gained prominence later in the twenty-first century in response to new technologies' emergence. This is presumably why the early domestic frameworks omitted explicit references to (informational) privacy, which at the time was primarily understood either as restriction of access to one's *private* (e.g. intimate) information or as individual control over their information, neither of which was the central concern of these frameworks.

Data protection then developed in a different direction as cross-border flows of data increased. These flows were increasingly affected by a patchwork of different national laws, which created uncertainty and inconsistency and led to efforts to harmonise rules internationally. This resulted in two major developments: namely, the non-binding OECD Guidelines and Governing the Protection of Privacy and Transborder Flows of Personal Data (adopted in 1980 and updated in 2013) and the legally binding treaty, the Council of Europe's Convention 108 for the Protection of Individuals with regard to Processing of Personal Data (adopted in 1981 and modernised in 2018 with 'Convention 108+'). Both frameworks sought to balance the dual goals of facilitating the free flow of information and safeguarding fundamental rights and freedoms, 'in particular' the right to privacy. In doing so, they established a close, instrumental link between data protection and privacy, portraying the former as a means to safeguard the latter. Simultaneously, they also introduced an ambiguity by implying an equivalence between the two (González Fuster, 2014: 253–256). This is especially evident in the OECD Guidelines, which consistently use the term 'privacy' rather than 'data protection' to frame the main *problematique* it responds to in the preamble (i.e. 'privacy risks') and to describe the relevant frameworks regulating the processing of personal data (i.e. 'privacy laws' and 'privacy enforcement authorities'). Notably, the Guidelines' explanatory memorandum recognises that 'data protection' is the preferred term in the EU and highlights how conceptions of privacy have '[g]enerally … broaden[ed]' from its 'traditional' understanding as '"the right to be left alone"' (OECD, 2023: 19). This suggests an understanding of privacy and data protection as largely equivalent,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

with the difference being primarily terminological. This exemplifies this Element's central claim: that the confusion and divergent interpretations surrounding the relationship between privacy and data protection arise in large part from terminological preferences across jurisdictions, as well as from differing (and evolving) understandings of privacy itself.

Another key international development often overlooked in historical accounts is the UN Guidelines on Computerised Personal Data Files (Bygrave, 2002: 33). Like the OECD Guidelines, these are non-binding, but they are also notably brief – just three pages, with no recitals, explanatory notes, or preamble. This brevity means they offer limited insight into the privacy–data protection relationship. Privacy is mentioned only once, in Article 9, which provides that 'transborder data flows' may occur freely where other countries 'offer comparable safeguards for the protection of privacy'. Some background documents on the Guidelines, such as the final preparatory report, refer to privacy as the main but not the only right protected by the Guidelines, in line with the language of other international frameworks. It is likely that the Guidelines were primarily intended to establish a shared (transatlantic) language rather than to set out an explicit or implicit position on the relationship between privacy and data protection. It is also worth noting that the emphasis on – or at least the explicit reference to – privacy across the three international frameworks is accompanied by a growing focus on the individual and their right to exercise control over personal information (Mayer-Schönberger, 1997: 226–227; see further Section 2.2 on these frameworks' substance). This is reflected in the set of rights these frameworks grant to data subjects, which aim to empower them vis-à-vis the processing of their personal data, such as the right to request access to or erasure of their information (as further delineated in Section 2.2). Arguably, the correlation between such rights and the increased visibility of privacy in these frameworks is not coincidental and suggests an implicit understanding of individual control as an integral aspect of privacy.

Subsequent developments at the EU level, however, deliberately decouple privacy and data protection. Data protection was initially regulated through the 1995 EU Data Protection Directive (DPD). The DPD was widely considered a 'market-born' framework, as it was enacted based on Art. 114 of the Treaty on the Functioning of the European Union (TFEU), which authorises legislation for the internal market. However, this market-based characterisation is overly reductive, as the choice of legal basis also reflected a treaty constraint: only with the 2009 Lisbon Treaty did the EU gain explicit competence to legislate for the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

'protection of individuals with regard to processing of personal data … and the rules relating to the free movement of such data' (Art. 16 TFEU, which reflects a balance between internal market and rights protection objectives on which the GDPR (replacing the DPD) was based; Bosua et al., 2025; Jančiūtė, 2017; Lynskey, 2015b). The Lisbon Treaty was also crucial in making the 2000 Charter of Fundamental Rights (CFR) legally binding. For the first time, the CFR enshrined a standalone right to data protection (Art. 8), distinct from the right to respect for private and family life (Art. 7). This distinguishes the CFR from other human rights frameworks, in which data protection is instead read into the right to privacy (see Section 3).

The inclusion of both rights in the now-binding CFR marked a clear shift in how the relationship between privacy and data protection was framed. Specifically, the GDPR, replacing the DPD, articulates its rights-based limb as the protection of the 'fundamental rights and freedoms of natural persons and in particular their *right to protection of personal data*' (Article 1; emphasis added), in contrast to the DPD, which instead singled out the 'right to privacy' as the 'particular' right protected (Art. 1). Strikingly, the GDPR refers to privacy only once, and merely *on a par* with other rights protected within the data protection *framework* (see Recital 4). Indeed, a key motivation behind the reform of the DPD through the GDPR was the European Commission's concern that individuals were losing control over their personal data (e.g. Recital 68 GDPR), prompting the introduction of a more extensive set of individual rights. This suggests that, at the EU level, data protection was understood predominantly as individual control over personal information. This interpretation is further supported by the drafting history of the right to data protection, as earlier drafts explicitly referred to informational self-determination (i.e. control over one's information), suggesting that this principle was likely the main driver underpinning the right (Clifford, 2024: 185; Bygrave, 2002: 119). Although the reference to informational self-determination was removed from the final text, it is reflected in various core data protection principles embedded in the GDPR (see further Section 2.2). Distinguishing data protection, understood in such control-based terms, from privacy implies, *a contrario*, that privacy was conceived in its traditional, narrower sense – namely, as a right to restrict others' access to one's information, in line with separation-based accounts. This reflects a more restrictive conceptualisation of (informational) privacy than the control-based understanding implied in the international data protection frameworks discussed above, resulting in a different understanding of how privacy relates to data protection.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Meanwhile, other data protection frameworks have been adopted at regional levels beyond the EU. These have often been overlooked in the literature comparing privacy and data protection, which tends to focus predominantly on the EU. But these regional instruments also illustrate – *and* contribute to – the ambiguous relationship between privacy and data protection. For instance, the (non-binding) OAS (Updated) Principles on Privacy and Personal Data Protection, the APEC Privacy Framework, and the (binding) ECOWAS Supplementary Act on Data Protection all appear to reinforce the close connection between privacy and data protection – whether by treating them as equivalent or by framing data protection as an instrument for safeguarding privacy. While the title of the OAS Principles explicitly refers to 'privacy *and* personal data protection (emphasis added)' – potentially implying a recognition that the two are different – the instrument's substance points in a different direction. It frames the purpose of the principles as 'establish[ing] effective rules for personal data protection that give effect to the individuals' right to privacy and demonstrate respect for their personal data', implying that data protection is conceived as a *means* of safeguarding privacy. Relatedly, the OAS Principles state that the term 'data', which defines their material scope (Section 2.2), was deliberately chosen over 'information' to indicate a broader scope aimed at promoting the greatest possible protection of 'privacy'. Somewhat confusingly, the introductory section of the OAS Principles includes a subsection on 'privacy', noting that the constitutions and laws of many member States guarantee data protection as 'distinct and complementary' to privacy and other rights such as personal dignity. However, read holistically, this appears to *describe* variations among Member States rather than introduce a conceptual separation between privacy and data protection within the Principles themselves. This reading is reinforced by the subsection's conclusion, which reverts to the notion of a general 'right to privacy' (OAS (Updated) Principles: 21) and states that privacy functions as an overarching category encompassing related rights such as data protection and dignity.

Going further than the OAS Principles, the APEC Framework refers *only* to privacy in its title. The preamble defines its dual goals as ensuring 'effective privacy protections' while avoiding barriers to information flows. Notably, the preamble presents the Framework's *raison d'être* as addressing the difficulty individuals face in 'retain[ing] a measure of control over their personal information'. When outlining obligations such as notice (i.e. informing individuals how their data is processed), the framework explicitly refers to 'informational self-determination' without introducing a separate right or concept, thereby presumably treating it as part

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

of privacy. These elements suggest that the drafters adopted a control-based understanding of privacy, thereby treating privacy and data protection as conceptually equivalent. A similar reading emerges from the ECOWAS Supplementary Act. Its preamble refers to human rights protection and the 'harmonization of the policies and regulatory framework of the Information and Communication Technologies sector', reflecting the dual aims of data protection frameworks. Notably, the preamble emphasises the 'urgency' of filling the 'legal vacuum generated by the use of internet' 'notwithstanding' national legislation on the protection of privacy and the free movement of information. This 'legal vacuum' could be read in two ways: either as implying that privacy alone is insufficient and needs to be complemented by data protection – suggesting a conceptual (and a legal) gap therebetween – or as pointing to the need to give concrete legal expression to data protection as a dimension of privacy. The latter appears more likely: Art. 2 states that the objective of the Supplementary Act is to protect 'privacy relating to the collection, processing, transmission, storage and use of personal data', subject only to the 'general interest of the state'. This phrasing, as in the OAS and APEC instruments, indicates that the Act treats privacy and data protection as closely intertwined, if not conceptually equivalent.

Conversely, the Ibero-American Standards – explicitly inspired by the GDPR, as indicated in their preamble – explicitly distinguish between 'data protection' and 'privacy' as separate rights. The Standards refer to the 'right to personal data protection' as a 'fundamental' right of a 'different' nature from the right to 'privacy'. They suggest that the right to personal data has 'its own characteristics and dynamics', aimed at safeguarding individual *control* over information. By framing data protection in control-based terms – and explicitly distinguishing it from privacy – the Standards imply a narrower understanding of privacy, possibly aligned with separation-based accounts. This echoes, to some extent, the conceptual division between privacy and data protection that is also implicit in the EU framework. As with the above frameworks, it is a particular conception of privacy that drives the framing of its relationship with data protection. However, to assess these varying framings, it is also necessary to understand what data protection *frameworks* – as the other element in the equation – encompass.

2.2 Core Data Protection Principles

This section delineates the content of data protection by examining the core data protection principles shared by the aforementioned frameworks.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

These frameworks vary both geographically and in terms of legal status, encompassing both binding and non-binding instruments. Among them, the (only) binding frameworks are Convention 108,[2] the GDPR, and the ECOWAS Supplementary Act.[3] This means not all of the frameworks examined here are what Greenleaf considers 'data privacy laws' in the sense of being legally binding treaties (2014: 8). Nevertheless, they represent the main international and regional efforts in data protection and are assessed here to identify the core elements that give concrete meaning to data protection (which, in turn, facilitates comparison with different conceptualisations of privacy).[4] At the outset, it should be noted that examining this broad range of data protection frameworks – adopted at different times and across different regional contexts – inevitably reveals divergences in terminology and formulation. Outlining core principles is therefore an exercise in approximation to identify general contours. Accordingly, the Element notes some nuances where appropriate and important – not to provide an exhaustive comparison, but to demonstrate that, notwithstanding certain variations, the frameworks are sufficiently aligned with one another to support a meaningful extraction of core principles.

Before discussing these core principles, it is first necessary to delineate the material scope of data protection frameworks. The material scope determines when these frameworks – and hence their core principles – apply. This scope pertains to the 'processing' of 'personal data'. Both terms are defined broadly across data protection frameworks, which illustrate the flexibility embedded in these frameworks to respond to new technologies as they emerge. Despite variations in the terminology used, their definitions are functionally similar. Personal data (or, e.g., 'personal information' under the APEC Privacy Framework, Art. II.9) refers to any information relating to an identified or identifiable individual. Importantly, this definition does not distinguish between 'private' and 'public' information – as understood in separation-based information privacy accounts (Section 1.1). It is rather odd, then, that the APEC Framework states it 'has limited application to publicly available

[2] Convention 108+ will enter into force once ratified by 38 Member States. Notably, Convention 108(+) are not self-executing instruments; each Member States needs to take measures within its domestic law to give effect to them.

[3] The binding force of the ECOWAS Supplementary Act notably varies by Member States' constitutional tradition (Orji, 2017).

[4] Further, some of these frameworks have significantly influenced the development of national data protection laws. For instance, the GDPR exemplifies the EU's 'Brussels effect' *par excellence*, while the OECD Guidelines significantly influenced various states such as Australia and New Zealand (Bradford, 2023, 2020; Clifford, 2024; Kirby, 1999).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

information' (Art. II.11). The accompanying commentary on this provision explains that notice and information provisions 'in particular' are 'superfluous where the information is already publicly available' and not directly obtained from the individual. This can be read to suggest that this provision on publicly available information does not delimit the Framework's material scope generally, but applies specifically to notice (i.e. transparency) obligations. This likely reflects the influence of traditional, separation-based conceptions of privacy, which tend to consider privacy extinguished when one's information is accessed by others; by equating privacy with data protection, the Framework adopts this restrictive tendency – even as it reflects broader, control-based understandings of privacy elsewhere (Section 2.1).

Another potential difference in the scope of 'personal data' across the frameworks concerns the breadth of identifiability, a constitutive element of the definition where information does not relate to an identified individual. Although identifiability has long been interpreted broadly at the EU level – largely through CJEU jurisprudence – recent case-law suggests a partial narrowing of this approach. In *EDPS* v. *SRB*, the Court held that pseudonymised information – data processed so that it cannot be attributed to a specific individual without additional information (Art. 4(5) GDPR) – is not necessarily personal data for all entities. Instead, information is personal data only for entities that have 'means reasonably likely [and, as per *Breyer v Bundesrepublik Deutschland*, lawful] to be used' to identify the person. At first sight, *SRB* may appear difficult to reconcile with earlier case-law such as *Breyer*, where the Court held that information may remain identifiable even if the necessary additional information is not 'in the hands of one person' (para. 43). This could be understood to offer a very broad conception of personal data, as in a context of increasing datafication and advanced re-identification techniques there will often be some third party holding identifying information. This understanding would substantially narrow the scope of anonymous data (i.e. data processed in a manner that the individual is no longer identifiable), which marks the outer limits of identifiability (and of personal data). Yet *SRB* can also be read as reaffirming the relative and subjective approach already implicit in *Breyer*. That case concerned whether a dynamic IP address constituted personal data for a website operator who did not themselves hold the identifying information (which was held by the internet service provider (ISP)). The Court found that the dynamic IP address could still be personal data, since the operator could reasonably and lawfully obtain the necessary information from the ISP, for example,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

in the context of a cyberattack and subsequent criminal proceedings. The mere existence of a third party holding identifying information was therefore not decisive; what mattered was the specific actor's realistic and lawful access to the additional information. This subjective approach to determining what constitutes personal data – and thus whether the GDPR applies – introduces a degree of uncertainty in the context of multi-actor processing environments and may narrow the regulation's material scope (see also Cobbe, 2026). The challenges embedded in this relative turn will assume increasing importance, especially in light of the European Commission's initial proposal of November 2025 to codify this approach, although a full examination lies beyond this Element's scope. It is sufficient to note here that this relative approach narrows – but does not eliminate – the potential gap between the EU framework and the (Updated) OAS Principles. This is because the latter excludes both anonymous and pseudonymised data from the scope of 'personal data'. While the OAS Principles do not define pseudonymised data, the use of a different term from anonymous data (which *is* defined in the Principles in similar terms to the GDPR) suggests that pseudonymised data is presumably intended to cover information that still allows re-identification (as under the GDPR). Excluding pseudonymised information from protection categorically reflects a narrower approach than the EU model, where such an exclusion will be context dependent. Yet given the ambiguities and loopholes inherent in the EU's relative turn, the practical difference between the two frameworks may be less substantial than it initially appears.

The second determinant of the material scope – processing – is also defined broadly across data protection frameworks. Processing (or, e.g., 'treatment' under the Ibero-American Standards, Art. 2(1)(i)) is deliberately framed broadly to cover any operation performed on personal data, including but not limited to its collection, storage, use, transmission, alteration, or erasure.[5] This expansive definition ensures that the core data protection principles apply throughout the data life cycle. It is therefore notable that some frameworks articulate specific principles only in relation to certain stages of processing. Namely, the OECD Guidelines (Art. 7) and the APEC Framework (Art. III.18) appear to limit the application of the collection limitation principle to the data collection stage only.

[5] Early data protection frameworks, such as Convention 108 and the UN Guidelines, limited their scope to *automated* processing, excluding or making optional the coverage of *manual* processing (Convention 108, Arts. 1 and 2(b); UN Guidelines, Art. 10). This restriction was removed in the modernised Convention 108+ (Art. 1) and is absent from later data protection instruments.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

This may reflect early frameworks' focus on regulating information *collection* (Bygrave, 2014; Clifford, 2024). Alternatively, it may result from imprecise drafting in the OECD Guidelines – later adopted by the APEC Framework – rather than an intentional restriction of the principle's scope. The focus on collection may have assumed that restricting collected data would naturally limit later uses, overlooking how minimisation applies across the processing life cycle. This latter interpretation is more consistent with the objective of these data protection frameworks, namely, to ensure that interferences with individuals' rights resulting from the processing of their personal data are no more than necessary for other legitimate rights and interests. It would be perverse if specific provisions, such as *collection* limitations, were taken literally and if similar limits did not extend to other processing activities, such as the storage or disclosure of personal data.

Data protection principles apply to personal data processing both in the private and public sectors, but some examined frameworks provide exceptions or limitations in national security contexts (see, e.g., OECD Guidelines, Art. 4; UN Guidelines, Art. 6; GDPR, Art. 2(2)(a); Ibero-American Standards, Art. 6; Twelfth OAS Principle; and so on). Regarding the subjects to whom data protection obligations apply, the primary addressees and duty-bearers are 'data controllers' (also referred to as 'controller' under Convention 108+, Art. 2(d), 'person responsible' under Ibero-American Standards, Art. 2(1)(c), or 'personal information controllers' under APEC Framework, Art. II(10)). On the other side are 'data subjects' who are the right-holders (also called 'holders' under Ibero-American Standards, Art. 2(1)(h) or simply 'individuals' throughout Convention 108+). Despite terminological variations, 'data subjects' refer to individuals whose personal data is processed, while 'data controllers' denote those who determine the purposes and means of that processing. Some frameworks also refer to 'data processors', who are the entities that process data on behalf of, and under the instructions of, data controllers. Given their subordinate role and generally limited direct obligations towards data subjects, data processors are not discussed further. For purposes of simplicity and consistency, the remainder of this Element will use the terms personal data, processing, data controller, and data subject.

In terms of substantive protections, the core data protection principles can be grouped into three main pillars: data subject participation, data controller obligations, and oversight. The first pillar includes principles imposing default obligations on data controllers. For example, the principle of lawfulness requires that the processing of personal data be based on

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

a legal basis. Some data protection frameworks provide an exhaustive list of legal bases, with data subject consent being the most common – though not the only – ground. The transparency principle requires that data subjects be provided with key information about their personal data processing in a concise and intelligible form. Such information includes, inter alia, the purpose, legal basis, and duration of processing. Transparency is closely linked to the fairness principle (referred to as loyalty in some frameworks: the Ibero-American Standards, Art. 15, and the First OAS Principle). Some instruments provide illustrative examples of fair processing, such as the obligation to avoid deception or fraud (ECOWAS Supplementary Act, Art. 24; APEC Privacy Framework, Art. III(18); and First OAS Principle). At the same time, they emphasise that these examples are not exhaustive, suggesting that fairness (or loyalty) entails a broader duty to act in a manner that respects the trust and legitimate expectations of data subjects (e.g. Ibero-American Standards, Art. 15; First OAS Principle).

Although the absence of a definition of fairness appears to be a deliberate choice to keep the concept open-ended, it also renders it inherently indeterminate. To complicate matters further, different layers of fairness seem to operate within data protection frameworks. These layers are not always easy to delineate (Clifford, 2022; for further details on the (European) scholarly literature unpacking fairness, see Clifford and Ausloos, 2018; Malgieri, 2020). Clifford's mapping of these layers (2022 and 2024), though rooted in the EU context, provides a useful lens for understanding fairness across different frameworks. First, fairness can be seen as a principle with both substantive and procedural aspects, overlapping with other principles in various ways. Procedurally, it is closely linked with transparency, equipping individuals with the information needed to make informed choices about their data. Substantively, it concerns the requirement to strike a 'fair balance between all interests concerned' (Convention 108+, Art. 5(1)). While explicitly articulated in some instruments, its substantive dimension is omitted in others such as the OECD Guidelines (Art. 7), where fairness appears process oriented. This substantive dimension overlaps with the broader role fairness plays in data protection frameworks. In this second layer, fairness functions as an overarching goal of the entire framework, operating as a system of checks and balances to achieve an appropriate equilibrium between competing rights and interests. Lastly, fairness may underpin – or at least form part of – the right to data protection, where such a right is provided in its own terms

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

(e.g. in the EU, in Art. 8 CFR), and is distinct from the broader data protection framework (e.g. the GDPR) itself (see further below on the connection between this right and fairness). The indeterminacy of fairness and its ambiguous relationship with other principles have produced diverse configurations across frameworks. Some treat lawfulness, transparency, and fairness as separate principles (e.g. Ibero-American Standards, Arts. 14–16), while others combine them in various ways (e.g. GDPR, Art. 5(1)(a)), which may be interpreted as one joint principle, two principles under the lens of fairness, or three distinct principles (Clifford, 2022, para. 14). Some frameworks pair lawfulness and fairness (UN Guidelines, Art. 1; OAS First Principles; OECD Guidelines, Art. 7; APEC Privacy Framework, Art. III.18; ECOWAS Supplementary Act, Art. 24), while others pair fairness and transparency (Convention 108+, Art. 5(4)(a)).

The principle of minimality requires that personal data be processed only to the extent necessary, measured against the specific purposes of processing. For the reasons set out in the discussion on 'processing' above, the minimality principle should be understood as applying to any processing operation, even where the relevant provisions enshrining it may sometimes refer specifically to the 'collection' of personal data (e.g. OECD Guidelines, Art. 7). This comprises three main prongs: purpose limitation (personal data must be processed only for specific and explicit purposes); data minimisation (only personal data necessary for those purposes should be processed); and storage limitation (personal data must be retained only for as long as needed to fulfil the stated purposes). Some frameworks articulate these prongs separately but within the same provision (e.g. GDPR, Art. 5(1)(b), (c), and (e); Convention 108+, Arts. 5(4)(b) and 5(1); and ECOWAS Supplementary Act, Arts. 25(1)–(4)). Others group some or all of the prongs together (e.g. Ibero-American Standards, Art. 18, and Third OAS Principle, which combines purpose limitation and data minimisation purposes). Some frameworks also combine aspects of minimality with other principles such as lawfulness and fairness (e.g. OECD Guidelines, Art. 7; APEC Framework, Art. III.18). Notably, not all frameworks explicitly provide for all three minimality sub-prongs. For example, storage limitation is absent from the OECD and APEC instruments. Similarly, the Ibero-American Standards do not provide storage limitations as a controller obligation but rather as part of the data subject's right to restrict processing when data is no longer needed (Art. 31). Nonetheless, the minimality principle is arguably implicit in these instruments through their inclusion of data minimisation, which applies to all processing operations, including storage.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

The data accuracy principle requires that personal data be accurate, relevant, and kept up-to-date in relation to the purposes of processing (e.g. Convention 108+, Art. 5(4)(d); UN Guidelines, Art. 3(a); GDPR, Art. 5(1)(d); OECD Guidelines, Art. 8; Seventh OAS Principle; ECOWAS Act, Art. 26; APEC Framework, Art. VI.21). By requiring data to be 'relevant' to processing purposes, the accuracy principle also reinforces minimality, ensuring only necessary and appropriate data is processed. The data security principle requires personal data to be adequately protected against, inter alia, unauthorised disclosure, tampering, exploitation, or loss. In the Ibero-American Standards, this principle appears as both the 'Safety Principle' (Art. 21) and the 'Confidentiality Principle' (Art. 23). Closely related to data security is the sensitivity principle, which calls for heightened safeguards for – or a default prohibition on – processing sensitive personal data, subject to limited exceptions such as explicit consent (e.g. ECOWAS Act, Art. 30; GDPR, Art. 9). Although sometimes presented as a standalone principle (e.g. the Ninth OAS Principle), it may be more accurately viewed as a rule applying to personal data requiring additional protection (e.g. GDPR Art. 9). The scope of sensitive data varies across frameworks but typically includes information on racial or ethnic origin; political opinions, religious, philosophical, or moral beliefs; trade union membership; health, sex life, or sexual orientation; and genetic or biometric data used for unique identification. To this list, Convention 108+ adds data relating to criminal offences, proceedings, and sanctions (Art. 6(1)), while the ECOWAS Act also covers administrative sanctions (Art. 1). Some frameworks adopt a broader definition of sensitive data, such as the UN Guidelines (Art. 5) and the Ibero-American Standards (Art. 2(1)(d)), the latter defining it as data 'refer[ring] to the intimate sphere of their holder, or whose undue use may cause discrimination or serious risk thereto'. The connection between the protection of sensitive data and the safeguarding of dignity, honour, and fundamental freedoms – as well as the prevention of discriminatory or harmful outcomes – is explicitly recognised in Convention 108+, Art. 6(2), and in the commentary to the Ninth OAS Principle. This link to non-discrimination is particularly pronounced in the UN Guidelines, which frame the sensitivity principle explicitly in terms of non-discrimination. The implications of this for the relationship between privacy and data protection frameworks are explored further in Section 2.3.

The second pillar – data subject participation – encompasses principles providing individuals with the tools to engage meaningfully in the processing of their personal data. This includes the principle of consent,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

which requires data controllers to obtain informed, explicit, voluntary, and revocable consent before processing personal data.[6] Consent is a common legal basis for processing and, as such, overlaps with the lawfulness principle (e.g. GDPR, Art. 6; Convention 108+, Art. 5(2); OECD Guidelines, Art. 7, where it appears under the 'Collection Limitation Principle'). Although the OAS Principles initially appear to treat consent (coupled with 'Transparency' under the Second Principle) as a separate principle, a closer reading shows it is simply one of several possible legal bases. The wording of the Second Principle refers to 'when processing is based on consent', implying consent is not always required, and the explanatory notes allow reliance on another legal basis if consent is not possible. The First Principle (Lawful Purposes and Loyalty) lists legal bases, including but not limited to consent, largely mirroring other frameworks. Thus, despite singling out consent and coupling it unusually with transparency, the OAS Principles' requirements on consent operate substantively much as in the other frameworks.

A second key principle under the participation pillar is data subject rights. These include the right to be informed about the processing of one's personal data, the right to request access to, rectification of, or erasure of that data, and the rights to object to or request restriction of its processing. Frameworks differ in how they provide for these rights: some, such as the GDPR and ECOWAS Supplementary Act, list them separately, while others group them, such as the OAS Principles (Seventh Principle); OECD Guidelines (Art. 13, 'Individual Participation Principle'); and Convention 108+ (Art. 9). Beyond these core rights shared across all instruments, some frameworks recognise two additional rights. The first is the right not to be subjected to solely automated decision-making that produces legal or similarly significant effects on the data subject ('the right against ADM') (see, e.g., Convention 108+, Art. 9(1)(a); GDPR, Art. 22; Ibero-American Standards, Art. 29).[7] Interestingly, the ECOWAS Act provides a different formulation of this right: the relevant provision (Art. 35) is titled 'Basis of a Court Decision' and includes a first clause prohibiting court decisions 'implying an assessment of the behaviour of an individual … based on … [automated processing] … evaluating certain aspects of their personality'.

[6] But note that the OAS Principles (p. 33) suggest that consent may be *implied* when the personal data is not sensitive and the purpose and method of collection are communicated transparently.

[7] The ambiguous framing had left it unclear whether this is a 'right' to be claimed by data subjects or a default *prohibition* on controllers. The CJEU resolved in *SCHUFA* (2023, para. 52) by adopting the latter view.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

The second clause provides a broader prohibition on any decision 'that has legal effect on an individual' based solely on automated processing to define a profile or evaluate aspects of personality. This appears narrower than provisions on the right against ADM elsewhere, as it omits decisions with non-legal but similarly significant effects and limits the scope to certain (yet vague) profiling purposes. The second 'additional' right is the right to data portability, which entitles individuals to receive their personal data in a structured, commonly used, and machine-readable format, and to request that it be transmitted directly to another controller (e.g. GDPR, Art. 20; Ibero-American Standards, Art. 30). Overall, although consent and data subject rights (both 'core' and 'additional') are often framed as enabling informational self-determination, the existence of legal bases beyond consent and the in-built limitations on data subject rights – such as when the controller's legitimate interests override – suggest that they more accurately support individual *participation* rather than full *determination* over personal data processing (Nolan, 2023: 125–131).

The third pillar – oversight – comprises two interrelated principles: accountability and supervision. First, the accountability principle requires data controllers to implement, and be able to demonstrate, measures ensuring compliance with their obligations. Data protection frameworks articulate these requirements in varying ways; accountability often implicates – and sometimes explicitly requires – data controllers to assess processing risks ex ante and adopt technical and organisational safeguards proportionate to the likelihood and severity of anticipated risks. Second, the supervision principle requires establishing independent bodies with effective powers, expertise, and resources to monitor and enforce data protection. These are often called 'data protection authorities' (DPAs).

Notably, this dissection of these core principles is not a neat one, as there is significant overlap, continuity, and complementarity therebetween. This means, importantly, that the three key pillars complement one another by allocating responsibilities to the main actors involved in ensuring compliance with data protection rules. For instance, data subject rights – many of which were introduced during the internationalisation of data protection principles – aim to empower individuals by enhancing their control over the processing of personal data. Bieker (2022) argues that this pillar represents the 'individual' face of data protection, which is complemented by its 'structural' dimension, that is, the first pillar that imposes default and general obligations on data controllers. This divide is not absolute, however, because exercising individual rights can drive structural change by exposing non-compliant practices to litigation

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

(as illustrated par excellence by high-profile cases brought by digital rights activists, such as the Schrems litigation: Ausloos and Dewitte, 2018; Clifford in Bosua et al., 2025). Nonetheless, the structural impact of data subject rights depends on individuals' ability, willingness, and resources to pursue them, often against powerful entities. For the same reasons highlighted by critiques of control-based accounts, the *actual* data subject does not always match the *assumed* profile. This is where the overlap between data protection principles becomes significant: this overlap means, for example, that data controllers should ensure accurate data processing *even* where data subjects do not or cannot exercise their rights to rectification. This means that data controller obligations protect 'even when nobody is looking' and even when no harm has materialised (Bieker, 2022: 59; Quelle, 2017). At the same time, data protection frameworks do not merely rely on the good faith of data controllers, and introduce a third actor: DPAs, responsible for overseeing processing systems. These DPAs may act upon requests and complaints from data subjects, but they also initiate investigations independently. Beyond protecting individuals, DPAs may perform a broader role by representing structural oversight of processing operations, with significant societal implications. The complementarity of these three pillars demonstrates that data protection frameworks go beyond granting individuals control over their information, requiring instead the establishment of a broader institutional infrastructure that safeguards systemic control over the flow of personal data (Basri, 2026: 6). These safeguards show that data protection explicitly takes into account and provides built-in mechanisms to respond to power asymmetries in the technological context. As such, they are relatively less unsettled by these asymmetries than mainstream conceptualisations of (information) privacy (i.e. separation- and control-based accounts).[8] Indeed, the structural components of data protection frameworks closely mirror the safeguards envisaged by power-based critiques of information privacy, and this suggests that scholars who adopt such perspectives but criticise data protection law as being overly focused on individual control may fail to appreciate these frameworks in their entirety.

In light of the above breakdown of the core principles, it is important to reflect on the uncertainty surrounding the conceptual foundations of the *right* to data protection and, consequently, its relationship with those principles. Although the right to data protection is explicitly recognised only in certain frameworks, understanding its conceptual foundations

[8] The emphasis should be on the relativeness of this observation, without claiming that data protection provides a foolproof tool to tackle emerging technologies.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

remains relevant even for frameworks that do not expressly provide for such a right. The overarching issue is whether there is – or should be – such a right, which is closely tied to the question of whether data protection offers any 'added value' compared to other pre-existing rights and freedoms, such as the right to privacy (see further Sections 2.3 and 3.3).[9] In EU literature – where most discussions surrounding the right to data protection have occurred, owing to its explicit provision in the EU CFR – the right has been conceptualised in two main ways: first, as a system of fairness-based checks and balances, and second, as informational self-determination. Hijmans and Dalla Corte fall into the former camp, arguing that the right to data protection can be perceived as a 'right to a rule'; 'a legal structure aimed at allowing individuals to claim that their data should be fairly and lawfully processed' (Dalla Corte, 2020; Hijmans, 2016: 66). This framing effectively treats data protection as a procedural framework that gives effect to rights and freedoms, rather than as a substantive right in its own terms (as Dalla Corte explicitly notes: 41). Differently, scholars such as Ausloos argue that this framing conflates data protection as a *framework* (per the GDPR) with data protection as a *right* (per Art. 8 CFR) (2020). Ausloos argues that while the former represents a regulatory framework, the latter constitutes a substantive right per se, one that pursues the independent objective of informational self-determination. According to this view, the right to data protection is not only about providing individual control through active rights (as embodied in the data subject participation pillar) but also about establishing a broader architecture and environment that enables individuals to maintain control over the processing of their personal information.

The differences between the two perspectives, however, may not be as substantial in practice as they initially appear. Under the first conceptualisation (data protection as a right to fair checks and balances), the right comes to represent the entirety of principles included under data protection frameworks. Under the second conceptualisation (data protection as a right to informational self-determination), the incorporation of the architectural dimension means that the right *also* encompasses many core principles within data protection frameworks, extending beyond those included in the data subject participation pillar. To illustrate, data minimisation and data security principles can also be seen as ways to limit interferences with individual informational self-determination, such as by ensuring that only the information necessary for a specified purpose

[9] See this notion of 'added value' in Lynskey, 2014.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

is processed and that it is not further disclosed to unauthorised parties. Although this second conceptualisation may appear more specific, hence narrower, than the first, it is not easy to separate the informational self-determination aspects of data protection frameworks from other rights-promoting elements within data protection frameworks; nor is it easy to disentangle these from the more market-oriented aspects of data protection, since many core principles pursue rights-based and economic goals jointly (see next subsection 2.3). These entanglements and overlaps across different principles mean that even under the second conceptualisation, uncertainty remains as to what, if anything, an understanding of the right as informational self-determination could exclude from the core principles of data protection. Accordingly, the ambiguities over the right's conceptual foundations – and, by extension, over which principles it encompasses – mean that the boundaries of the right and its relationship to core principles under data protection frameworks are not clearly marked. Consequently, even scholars who explicitly discuss the right to data protection often turn to data protection frameworks themselves when comparing data protection with privacy.[10] Accordingly, the following subsection also refers to data protection principles when comparing data protection with privacy, while returning to the question of whether there is or should be a right to data protection when considering the added value such a right would bring to *pre*-existing rights and freedoms.

2.3 Revisiting the Conceptual Relationship between Privacy and Data Protection

Building on the multifaceted understandings of (information) privacy and data protection developed thus far, the relationship between the two can now be revisited in a more nuanced manner. This analysis considers the two possible ways in which the relationship between data protection frameworks and privacy can be articulated, as reflected in the scholarship: first, by viewing privacy and data protection in binary and contrasting terms; and second, by viewing data protection as pursuing a plurality of objectives, with privacy being one of the main objectives. Whereas the first view treats privacy and data protection as serving distinct and potentially opposing functions (albeit ones that may still complement each other), the second understands them as sharing similar components and functions,

[10] One difficulty with this approach in EU law is using the data protection framework (GDPR; secondary law) to define the right to data protection (Art. 8 CFR; primary law). This is odd, as under EU law secondary laws are enacted to give effect to the rights protected under primary law and therefore do not determine the latter's content.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

such that they overlap without being identical. The following discussion demonstrates that the second model – framing data protection and privacy as 'heavily overlapping' yet non-identical – is the most persuasive, while also showing that this framing does not fully resolve but shifts the ambiguity from the *nature* of their interaction to the *extent* of their overlap.

The first view, which considers privacy and data protection as distinct (yet possibly complementary), rests on a series of interconnected contrasts defining their relationship ('the distinction model'). For instance, de Hert and Gutwirth argue that privacy and data protection are both necessary to limit State power but serve different functions: privacy provides an 'opacity tool' by 'setting normative limits' on the reach of the State's power, whereas data protection offers a 'transparency tool' that 'regulat[es] and channel[s] necessary/reasonable/legitimate power' (De Hert and Gutwirth, 2016: 510; see also Tzanou, 2013: 97). The authors' focus on the State-as-controller is presumably due to the law enforcement context in which they were writing, but their account also conceptualises privacy and data protection more generally beyond this setting. This contrast between opacity and transparency leads to a series of related distinctions: privacy operates as a *prohibition* entailing *negative* obligations, whereas data protection functions – at least as 'a general rule' – as a *legitimising* framework imposing *positive* obligations (De Hert and Gutwirth, 2016: 520; see further on the legitimising versus prohibiting nature of data protection in the EU context in González Fuster and Gutwirth, 2013). These features characterising their nature also cascade into temporal qualities: Rodotà suggests, for instance, that privacy is 'static', aimed at preventing interferences at specific moments, while data protection is 'dynamic', setting out rules for data processing throughout its life cycle (2009: 79–80). Dalla Corte offers another contrast, arguing that privacy is a substantive right (exemplifying a 'right[] that are created to protect and uphold interests considered important') while data protection is a procedural right/framework (exemplifying a 'right[] that appear at a later stage, setting the conditions through which substantive rights are implemented') (2020: 41; see also Tzanou, 2013: 90).

Notably, these contrasts hold true only insofar as one selectively focuses on specific facets of privacy and data protection. A more nuanced understanding of both concepts helps to illustrate the fragility of these contrasts. For instance, a holistic view of the core data protection principles reveals that the distinction model overlooks – or at least oversimplifies – important aspects of data protection in order to sustain these contrasts. De Hert and Gutwirth themselves recognise these limitations,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

noting that although data protection operates primarily as a transparency tool, exceptions exist (2016: 520). These exceptions are particularly evident in the sensitivity principle, which establishes either default prohibitions on processing sensitive personal data or imposes strict conditions on processing such data. Minimality can likewise be seen as a prohibitory rule, forbidding the collection and storage of personal data beyond that which is necessary to fulfil the specified purposes (Bygrave, 2001: 280). While the contextual nature of these principles admittedly limits their prohibitory force – since their applicability, including determinations of what amount of personal data is 'necessary' for a given purpose, is made on a case-by-case basis, and data controllers, the duty-bearers, are themselves the primary actors making these decisions (see relatedly Clifford, 2024: 135–174) – the better view is that data protection remains both prohibitory and legitimising. Instead, these principles can be seen as a means of ensuring that processing occurs proportionally, mirroring the legal protection of the right to privacy, which is also not an absolute right and can be lawfully restricted to the extent necessary and proportionate (see further Section 3). The recognition that data protection principles also include prohibitory elements further means that data protection (also) entails obligations to refrain from certain conduct. Indeed, most data protection principles arguably have *both* negative and positive dimensions. To exemplify, data security not only requires that data be not disclosed to unauthorised parties (a negative obligation) but also mandates active steps to prevent access by such parties and ensure that adequate measures and architectures are implemented to preserve confidentiality and integrity (reflecting positive obligations to 'protect' and 'fulfil'). The final contrast offered in the distinction model – the procedural versus substantive nature of privacy and data protection – is revisited below when discussing data protection's added value.

Similarly, on the 'privacy' end, the distinction model relies on a narrow understanding of (information) privacy to construct and maintain the contrasts it proposes. Although proponents of this view do not always define privacy explicitly, their references to opacity suggest that they understand it in separation-based terms. This allows them to distinguish data protection frameworks as doing more than – or sometimes even the opposite of – simply restricting the sharing of private information. However, as discussed in Section 1, a nuanced understanding of privacy should not be limited to separation-based accounts but must also incorporate control-based accounts and, at least, some of the insights offered by power-based critiques. All three perspectives shed light on key features of privacy, and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

indeed, each is reflected in the different components of data protection frameworks. The overlap between separation-based accounts of privacy and data protection is evident in the sensitivity principle and other 'prohibitory' aspects of data protection. Control-based accounts of privacy are reflected in the data subject participation pillar in two ways. First, in the criteria for valid consent, which are designed to ensure that, where consent serves as a legal basis for processing, it represents the data subject's genuine and informed control. Second, in the 'micro-rights', which provide data subjects with tools to exercise control throughout the processing life cycle (Lazaro and Métayer, 2015: 15–16). Notably, scholars such as Lynskey draw on these control-based elements to distinguish privacy from data protection, which can be read as reflecting a separation-based, rather than control-based, understanding of privacy. This becomes evident when Lynskey observes, for instance, that the strict conditions attached to consent under data protection 'do not stem from *traditional* privacy concerns' (emphasis added) but instead arise from a recognition that, in such settings, individuals 'are not, de facto, in control of their personal data' (Lynskey, 2015b: 189–190). This suggests that the objective served by consent here is not 'privacy' but 'individual control' (see also Tzanou, 2013: 89). Whilst consent would indeed not sit easily with separation-based accounts – since they would view any processing of personal data as an interference with, rather than an exercise of, information privacy – control-based accounts, which focus on data subjects' *subjective wishes*, necessarily require that any consent for data processing be given voluntarily.

Lastly, recognising the limitations of individual control in power-asymmetric settings (Section 1.2), data protection frameworks are built on pillars that accommodate both 'individual' and 'structural' components. The resulting focus on broader systems of information processing resonates with key contributions of power-based critiques to information privacy conceptualisations. In particular, the structural dimension of data protection – inter alia through a set of ex ante obligations on data controllers – aligns with these critiques by ensuring that information processing should be regulated at broader levels, even in the absence of a demonstrable impact on an individual. At the same time, a fundamental difficulty in comparing and contrasting power-based critiques of privacy with data protection is that, as explained in Section 1.3, such critiques often extend beyond (information) privacy, making it difficult to determine where their observations on the right to privacy end and where other rights and interests begin. Sometimes, they directly talk about privacy and data protection in same terms, reflecting jurisdictional

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

terminology preferences. Ultimately, the recognition of the broader conceptualisations of (information) privacy *and* the multidimensional nature of data protection demonstrates that the supposed contrasts between privacy and data protection are not only over-simplistic but also inaccurate, even as general framing tools.

This paves the way to assess the second framing of the relationship between data protection and privacy as overlapping yet non-identical. The latter aspect, that the two cannot be 'identical', is relatively straightforward to establish when one recalls that under examination here are data protection *frameworks*, which are instruments that expressly identify their objective as the protection of *a range* of rights and freedoms including but not limited to privacy, as well as certain *economic objectives*. This (rights-versus-market-based) duality manifests itself not only in the normative values data protection frameworks protect but also in the substance of their core principles. The 'market-based' end of this duality is most visible in how data protection principles legitimise and enable the free flow of information for grounds other than – and sometimes even against – data subjects' subjective wishes. For instance, the lawfulness principle permits the processing of personal data without the data subject's consent, including even where processing is not in their interests, provided that controllers can demonstrate a legitimate aim, such as pursuing economic interests through direct marketing which does not override data subjects' fundamental rights and freedoms (e.g. GDPR, Art. 6(1)(f) and Recital 47). Likewise, data subjects' exercise of their micro-rights may be restricted, inter alia, where controllers can invoke overriding legitimate interests, which may include their commercial objectives (e.g. GDPR, Art. 6(1)(d)). These examples demonstrate that an overarching principle of fairness underpins data protection frameworks as a fundamental premise, but fairness operates not solely to protect data subjects' rights; it also functions pluralistically to safeguard other interests, such as data controllers' economic interests (Clifford, 2024: 17; Bygrave, 2002: 282).[11]

[11] This comparison between the objectives of data protection frameworks and privacy may be objected to on the basis that human rights frameworks enshrining the right to privacy (*also*) enable the lawful pursuit of a range of other rights and interests. This can be seen in the fact that the right to privacy is not an absolute right and may be qualified to protect a range of different interests, such as the economic objectives of a state or national security (e.g. Art. 8(2) of the European Convention on Human Rights). Yet, there are important differences. The right to privacy does not aim to protect broader (and multiple) interests such as national security or economic objectives; rather, it renders interference with the right to privacy permissible for these purposes where certain conditions (e.g. proportionality) are met (see further the discussion of the jurisprudence on the right to privacy by human rights courts in Section 3). In this regard, the protection of other rights and interests emerges only implicitly/indirectly under privacy, in the sense that it results from

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Yet the duality and simultaneity of the objectives pursued under data protection mean that it is not always easy to disentangle the rights-based and market-based elements of these frameworks, which may sometimes overlap. Even those elements that seemingly fall at the latter end (market-focused components of data protection) – and would therefore be relatively easier to separate from the right to privacy – are often interwoven with rights and interests that could also be captured under (broader conceptions of) privacy. A frequently discussed example in this context is the right to data portability, although, as noted, this right is not universally recognised across all data protection frameworks. The ambiguous nature of the right within the economic-versus-rights-based duality is illustrated by the different ways it has been understood in the literature: whilst Lynskey, for instance, suggests that data portability falls within data subject micro-rights, forming part of data protection's overarching aim to 'allow individuals to better determine how their data is processed, by whom, and for what purposes' (2014: 591) (which provides an interpretation that may also bring data portability within control-based accounts of privacy), others such as Cormack (2016) discuss data portability primarily as a remedy aimed at enabling consumers to switch service providers to enhance competition and foster innovation. In a way, the right does both, as it fosters competition within the market for higher privacy and data protection standards, between which the data subject, as a consumer, can choose (see below on what other safeguards data protection may add compared to privacy). Data accuracy depicts a similar duality (and ambiguity). On the one hand, this principle can support certain understandings of privacy by ensuring that only accurate and contextually relevant personal data is processed, thereby preventing the circulation of irrelevant information that could undermine personal control or lead to privacy intrusions. On the other hand, data accuracy also serves broader interests. As Bygrave notes, 'it [also] breaks down into a multiplicity of interests …

conduct not amounting to a breach of the right, rather than from their pursuit as such. Put differently, these are not objectives pursued by the right to privacy, but pragmatic and necessary concessions made from the right under certain circumstances (further on the legal protection of the right to privacy, see Section 3). This differs from data protection frameworks, whose historical evolution and substantive content demonstrate the explicit and joint pursuit of multiple aims (in addition to the right to privacy). Admittedly, this comparative observation between privacy and data protection is a natural result of them being non-equivalent subjects of comparison (of a *right* with a *framework*). This circles back to the limitations of using the data protection framework (rather than the right to data protection) as the object of comparison, which itself stems from the ambiguities surrounding the conceptual foundations and content of a self-standing right to data protection. These ambiguities are set out at the outset of this section, and the question of a distinct right to data protection is revisited further below in this subsection.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

that have little direct connection to privacy-related values' (2001: 281), such as enhancing efficient data processing by reducing operational risks and costs that might arise from inaccurate or outdated data. The simultaneity of different interests pursued under data protection frameworks thus makes it difficult to determine which of their multiple elements fall within, and which fall outside, the right to privacy.

These difficulties are further compounded by the fact that data protection frameworks pursue multiple (human) *rights*, whose boundaries with information privacy are also not always clear. One such right, frequently and explicitly pursued under data protection frameworks, is the right to protection from discrimination. This right manifests most clearly in the sensitivity principle, which the UN Guidelines explicitly label as the 'non-discrimination principle'. The categories of information protected under this principle broadly mirror, but are not identical to, the prohibited grounds of discrimination, such as information concerning ethnicity, religion, or sexual identity. As some frameworks explicitly highlight, protecting sensitive data aims both to pre-empt and reduce the risks of discrimination while also safeguarding information in the most intimate realms of individuals, thereby overlapping with privacy interests emphasised in separation-based conceptualisations. Another component aimed at protecting against discrimination is the right against ADM. This right seeks to prevent the de-individualisation of persons by prohibiting significant decisions about individuals that are based not on their own characteristics or behaviour, but on attributes assigned to algorithmically profiled groups. This overlaps with, yet goes beyond, protection against discrimination. Individuals may be grouped based on characteristics not covered by discrimination law (such as age, ethnicity, or sex), but rather on specific behaviours, for example, the websites they visit. Moreover, these groups are generated through correlations of multiple, often opaque factors, undermining the requirement to establish a clear link between a protected ground and unjustified differential treatment as required under discrimination law. Crucially, the right against ADM *also* appears to extend beyond (information) privacy. Although the initial collection of data that feeds into ADM systems may raise privacy concerns, none of the conceptualisations of information privacy offer a satisfactory account of how the act of making and applying algorithmic decisions itself constitutes a *privacy* issue (Section 1.2). Likewise, while power-based critiques address ADM more explicitly by acknowledging the risks of biased and potentially discriminatory outcomes, they tend to treat these risks as *consequences* of privacy violations rather than as *constitutive elements* of privacy per se.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

This brings us back to the difficult question posed at the beginning, which has no easy answers: is data protection merely a means to further a plurality of objectives protected by pre-existing rights, freedoms, and regimes, one of which is privacy, or does it have an 'added value' of its own? Such an added value would mark the area where neither privacy nor another protected right or interest could extend and justify, or call for a space to be carved for, a self-standing *right* to data protection. The analysis of the right against ADM is a good example, explored functionally here to illustrate that there might be an argument for such a space. At the same time, this example also demonstrates the difficulties in then delineating the boundaries between privacy, data protection, and other interests and rights also served by them, precisely because of the uncertain foundations of all these rights and protections. As mentioned above, scholars who argue that data protection has its own independent interest often point towards informational self-determination. Like Ausloos, Lynskey argues that the distinct addition of the right to data protection, alongside the right to privacy, is that the former grants individuals more rights over a broader range of information, thereby enabling informational self-determination. This allows individuals to better determine how their data is processed, by whom, and for what purposes. In turn, this facilitates, first, selective self-representation, whereby individuals can choose which facets of their identity they share with different audiences; and second, the structural mitigation of power asymmetries in the context of information processing (2014: 591). The descriptive aspect of this position is difficult to challenge; the above discussion makes clear that data protection can regulate forms and types of information processing that cannot be fully captured by privacy or by another right such as protection from discrimination. Yet the normative observation that informational self-determination distinguishes privacy and data protection (both as rights) may be better qualified and caveated, because privacy, too, can be conceptualised in terms of individual control and thus can serve much of the two aspects highlighted by Lynskey. Instead, it might be claimed that both privacy and data protection can serve informational self-determination, but data protection has an added value because it serves informational self-determination *more* comprehensively, both in terms of the categories of information it covers and the tools it provides to secure such control.[12]

[12] Note however that Lynskey (2014: 573) concludes, similarly, that the right to data protection 'offers individuals enhanced control over their personal data'

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

This supports the second model categorising the relationship between privacy and data protection as non-identical yet 'heavily overlapping' (see similar conclusion in Lynskey, 2015: 90). Yet this model is the most persuasive since it shifts the ambiguity towards identifying the sphere of overlap. As this Element shows, this task becomes increasingly difficult the more one focuses on broader conceptualisations of information privacy and adopts a more multifaceted view of data protection. One may therefore need to turn to the law on the right to privacy to better understand the concrete differences that have emerged in practice between privacy and data protection, as Section 3 now does. But, as will be seen, the law is often driven, constrained, and muddled by these conceptual ambiguities, which are not merely abstract debates but have tangible implications – albeit often implicit – for how the law has developed and may continue to develop (see relatedly Clifford, 2024: 208).

3 The Relationship between the Right to Privacy and the Core Data Protection Principles under Human Rights Law

This final section now tests the conceptual argument built – that privacy and data protection frameworks heavily overlap but are non-identical, with the contours of their relationship shifting based on how each is understood – under human rights law.[13] It does so by comparing the protections provided under the right to privacy to those offered under data protection frameworks, first by comparing their material scope (i.e. *when* protections apply) and second by comparing their substantive protections (i.e. *what* protections apply). The high-level framing of the right to privacy across human rights treaties means that both of these aspects are developed through jurisprudence interpreting this right at the relevant forums, namely the European Court of Human Rights (the European Convention on Human Rights (ECHR), Art. 8),[14] the Inter-American Court of Human Rights (American Convention on Human Rights (ACHR), Art. 11),[15] and the Human Rights Committee

[13] It is important to note that privacy is not only protected as a human right; domestic laws also provide for the protection of privacy in various ways, such as through national statutes regulating surveillance. This means that the protection of privacy under human rights frameworks is complemented by other legal protections at the domestic level (whose exploration goes beyond the scope of this Element which takes an international perspective).

[14] Art. 8(1) ECHR provides 'Everyone has the right to respect for his private and family life, his home and correspondence'.

[15] Arts. 11(1) and (2) ACHR provide, respectively, 'Everyone has the right to have his honor respected and his dignity recognized' and 'No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

(International Covenant on Civil and Political Rights (ICCPR), Art. 17).[16] Understanding the legal overlap between privacy and data protection is also crucial for assessing whether existing protections under data protection frameworks can be accommodated within the right to privacy (or other relevant human rights, such as protection from discrimination, which is also briefly addressed below), or whether a distinct (human) right to data protection may be justified.

Some initial methodological remarks are due on how this jurisprudence is used to unpack the material scope and substantive protections of the right to privacy. First, the discussion below excludes the African Charter on Human and Peoples' Rights, as that is the only major human rights treaty that does not explicitly guarantee a right to privacy.[17] Second, the ECtHR's jurisprudence is treated more extensively than other bodies of case law because the Court has developed the most elaborate jurisprudence on information privacy, and its case-law has been influential in shaping that of other jurisdictions (on factors that determine the level and direction of cross-fertilisation between IHRL bodies, see Abrusci, 2023). Third, the human rights jurisprudence discussed below also includes the HRC's outputs, drawing on, first, its Views, where the HRC assesses compliance with the ICCPR based on individual complaints, resembling judicial reasoning; second, General Comment (GC) No. 16, which provides a general interpretation on the right to privacy; and third, Concluding Observations, where the HRC assesses States' compliance with the ICCPR based on reports they submit and makes further recommendations. While these outputs are not legally binding on States Parties, they form part of UN human rights jurisprudence. Since States explicitly created this body to interpret the ICCPR, in which it has extensive expertise, its outputs carry significant persuasive weight unless expressly objected to by a State Party (Sitaropoulos, 2015). Fourth, some IHRL treaties refer to 'privacy' (ICCPR), while others use 'private life' (ECHR and ACHR). This terminological difference likely reflects linguistic variation between English and French (privacy vs *vie privée*, translated as 'private life') and has not affected how the right is interpreted by IHRL bodies. The discussion below follows the terminology of the respective treaties examined, while using 'privacy' for broader observations (using the term to refer to *information* privacy, consistent with Section 2).

[16] Art. 17 ICCPR provides: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation'.

[17] But on the emerging role of privacy in the African system, see further (Ayalew, 2022).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Finally, it is important to highlight that IHRL sets out the obligations of the States as the main subjects of IHRL, whereas data protection frameworks apply to both public and private actors. This itself is a crucial difference regarding the applicability of both frameworks.

With these methodological considerations in mind, the following analysis explores the relationship between privacy and data protection through the conceptual observations offered above. The order of analysis – the legal discussion following the conceptual analysis – is deliberate. The right to privacy is framed at a high level (like other human rights) and has not always been interpreted or applied by human rights bodies in consistent, clear, or sophisticated ways. This necessitates applying a theoretical lens to human rights jurisprudence to make sense of it, specifically, to understand why privacy has evolved in relation to digital technologies as it has. In this regard, Sections 3.1 and 3.2 compare the material scopes and substantive protections of privacy and data protection, respectively, identifying their overlaps and non-overlaps, and exploring why the latter is so difficult to delineate. Section 3.3 concludes with reflections on what these observations reveal about the added value of data protection.

3.1 Material Scope

A clear comparison of the material scopes of privacy and data protection is encumbered by the fact that human rights bodies do not always or clearly distinguish between when the right to privacy is *engaged* and when it is *interfered with* (Lynskey, 2014: 583). Only the former reveals its material scope, whereas a finding that the right to privacy was not interfered with may mean either that the right was not engaged at all or that it was engaged but not interfered with. Despite this ambiguity, the jurisprudence still offers some sense of the scope of information privacy. It illustrates that the material scope of (information) privacy is more restricted than that of data protection, although the gap between the two has been narrowing as human rights bodies have become more willing, albeit only partially, to embrace broader conceptualisations of privacy (Lynskey, 2014).

This evolution is best illustrated by the ECtHR's case-law, which has long engaged with the informational dimension of privacy. Early cases delineated the material scope of the 'private life' through a public–private dichotomy, reflecting the traditionalist separation-based accounts. For instance, in *Herbecq and the Association 'Ligue des droits de l'homme'* v. *Belgium* (1998), the European Commission of Human Rights (which filtered and referred petitions to the ECtHR until its abolishment in 1998)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

found the complaint against unregulated police CCTV surveillance manifestly ill-founded, as the surveillance concerned 'essentially public behaviour' and did not render captured information 'available to the general public'. This approach has not been maintained in later cases and, in any event, is also inconsistent with the jurisprudence being developed by the ECtHR during that period. Notably, the Court has come to firmly recognise – which it now reiterates as a general principle under Art. 8 – that 'it would be too restrictive to limit the notion [of private life] to an "inner life" … and to exclude entirely the outside world not encompassed within that circle' (*Niemietz* v. *Germany*, 1992, para. 28). It holds that respect for private life 'must also comprise to a certain degree the right to establish and develop relationships with other human beings' (*Niemietz* v. *Germany*, 1992, para. 29), recognising the relational aspect of privacy. This recognition has expanded the scope of information covered under privacy to include business-related information obtained in the workplace, since 'it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world' (*Niemietz* v. *Germany*, 1992). As Section 1.1 explains, separation-based accounts can also accommodate relational privacy by encompassing individuals' social (private) lives. This decision illustrates this: the Court includes professional information within the scope of the right to private life because working lives (and information pertaining to/emanating from them) are an aspect of individuals' interpersonal relationships with others. Simultaneously, the decision also echoes, to some extent, a control-based understanding of privacy, as it shifts the focus away from the nature or content of information towards the individual's ability to manage their self-presentation across different contexts for the purposes of developing and maintaining various relationships, albeit provided that these pertain to close, personal relationships within one's private sphere of life.

This control-based understanding of privacy is most clearly reflected in *Von Hannover* v. *Germany (No. 1)* (2004), which concerned the publication of Princess Caroline of Monaco's photos in German magazines. The Court suggested that privacy includes 'the individual's right to control the use of [their] image[s]' and exists 'even in the sphere of the relations of individuals between themselves' (paras. 57, 72). The nature of photos against which this right to control was articulated is significant: they depicted the Princess engaging in everyday activities such as horseback riding, shopping, skiing, leaving her house, playing tennis, or tripping over an obstacle at a beach club. Admittedly, some of these

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

images could be regarded as 'private' insofar as they pertained to her personal, intimate life (Section 1.1) – for instance, images taken around her house (which could be considered private by 'context', as they were obtained in a climate of harassment by waiting near her most private space (home)) or images of her interacting with a friend (which could be considered as part of her private life regarding her personal relationships). Yet, this cannot be said for *all* the photos, such as those showing her shopping in a market or cycling, which separation-based accounts would struggle to classify as private, since they were intuitively private neither by content nor by context, being taken in publicly accessible spaces. While the Court acknowledged these were scenes from her daily life in public spaces, it nevertheless characterised them as 'very personal or even intimate "information"' (para. 59). This is a clear 'mischaracterisation of the images', which highlights a fundamental tension in the Court's reasoning (Hughes, 2009: 161). Although the Court applies a broader, control-based understanding of privacy – focused on managing access to personal information about one's public image – it implicitly remains attached to more traditional, separation-based accounts that associate privacy with intimate or secluded information. To be sure, and as explained in Section 1, separation- and control-based accounts are not necessarily incompatible, in the sense that the latter may regard control over information as exercisable only in relation to 'private' information. However, what is striking in this decision is the Court's reluctance to openly articulate what it is in fact doing, namely, protecting essentially public information (i.e. to recall, information which is not private by nature and which is available from public domains).

Other jurisdictions also suggest that the scope of the right to private life extends beyond traditionally private information, though similar tensions underpin some of these approaches. One example is the IACtHR's decision in *Fontevecchia and D'Amico* v. *Argentina* (2011), which concerned the publication in a newspaper of the existence of an illegitimate son of then-President Carlos Menem. Similar to the 'right to control the use of [one's] images' articulated by the ECtHR in *Von Hannover*, the IACtHR suggested that privacy encompasses the 'control of the dissemination of personal information to the public' (para. 48). The IACtHR did not elaborate further on this statement, which at face value hints at a broader scope than 'private' information, akin to that of 'personal data' that defines the material scope of data protection frameworks (Section 2.2). Notwithstanding this, a closer look at the case's facts suggests that the Court's seemingly broad statement should be taken with caveats. In

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

particular, the information at issue concerned reputationally damaging content. Therefore, despite the Court's seemingly broader articulation of privacy as control over the dissemination of 'personal information', it was arguably referring to a narrower category of highly private information, namely humiliating content whose publication would expose it to very large audiences. The information at stake in this case also possibly suggests that, when discussing a right to control the dissemination of one's information to the public in this context, the Court may have had in mind the protection of honour and dignity, which are explicitly protected under Art. 11 ACHR alongside the right of private life. This decision reveals a tension between the Court's rhetoric and its application that is similar to that in *Von Hannover*, but in the opposite way: the IACtHR articulated a broader scope of privacy protection than it applied in this case. Most recently, *CAJAR* v. *Colombia* (2023) went much further by articulating a notion of control as informational self-determination exercisable vis-à-vis 'personal data', which the Court defined in the same terms as 'personal data' under the OAS Principles. However, it is difficult to use this case as a basis for comparing the material scope of privacy and data protection, as the Court grounded informational self-determination jointly on *various* rights, as discussed further below.

In other cases where human rights jurisprudence has explicitly deconstructed the private/public distinction, it has nevertheless required additional factors – such as the extensiveness of processing operations – to bring public information within the scope of the right to privacy. In cases such as *Rotaru* v. *Romania* (2000) and *PG and JH* v. *UK* (2001), the ECtHR affirmed that public information (specifically referring to information publicly available, i.e., obtainable from public spaces) falls within the scope of the right to private life, 'even where the information has not been gathered by any intrusive or covert method' *provided that* it is 'systematically [or permanently] collected and stored in the files held by the authorities' (paras. 59 *Peck* v. *UK* (2003), 43 (*Rotaru*), and 57 (*PG*)). Other human rights bodies have not made explicit determinations vis-à-vis public information. However, at the UN level, the HRC's concluding observations and reports by the UN High Commissioner for Human Rights (OHCHR) seem to confirm that 'public' information can fall within the scope of the right to privacy only where processed systematically – a criterion which they express either explicitly or implicitly (by virtue of references to and problematisations of the *scale* of surveillance practices: see, e.g., HRC, 2016, para. 32; OHCHR, 2022, para. 43). The notion of 'systematicness' is undefined, but presumably it refers to data

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

being processed either on a large scale or in methodical/structured ways (i.e. as part of a system). This expansion of privacy protections to cover publicly available information that is processed systematically suggests that human rights bodies are becoming less concerned with the content of the information itself and more with the aggregation of seemingly trivial data, which can be used to develop detailed profiles of individuals, echoing power-based perspectives on privacy. Nevertheless, the focus on the nature of the information is not entirely lost: the added criterion of systematicness imposes a higher threshold for public information to fall within the scope of privacy, in contrast to the material scope of data protection, which applies to any processing of personal data regardless of its scale. This approach can be regrettably restrictive because it may result in the exclusion from privacy's scope of public information that is not systematically or permanently *processed by the State Party at the time of the Court's assessment*, even if that same data is later shared or combined with other datasets to generate detailed insights about individuals, including by other actors. This restrictive focus under IHRL – both in actoral and temporal terms – suggests that it does not fully capture the broader infrastructures of information processing and the role of multiple actors in generating privacy breaches. This contrasts with the data protection approach, where personal data is defined through the concept of identifiability, which includes a relational element: information that may not identify an individual on its own but could do so when combined with other information held by different actors. This recognises and accounts for the presence and capacities of various actors in determining the material scope of data protection.[18]

The foregoing analysis demonstrates that the material scopes of (information) privacy and data protection are distinguished by the additional contextual considerations that limit the former, though not always consistently (as in *Von Hannover*, where all photos were deemed intimate despite depicting scenes from public life) or desirably so (as in *Rotaru*, where the treatment of 'public' information may be overly restrictive). Two apparent anomalies in the jurisprudence, challenging this general

[18] This distinction between privacy and data protection regarding private versus public information, however, requires a caveat. As Section 2.2 explains, the APEC Framework also states that it has limited application to publicly available information. This means that even where public information falls within the scope of personal data, the material scope of that Framework may exclude the application of certain data protection principles (e.g. in APEC, the transparency principle) – an exclusion that can have a similar effect to removing such information from the material scope in the first place (at least in relation to the operation of those principles).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

position, require addressing. The first is the ECtHR's frequent claim that its broad interpretation of (information) privacy aligns with the definition of 'personal data' under Convention 108. Yet this claim is largely rhetorical. As discussed, the Court's jurisprudence shows a consistent reliance on additional contextual factors when recognising privacy interests in non-private information – specifically, a link to an individual's private life, including close personal relationships (as in *Niemietz*), or systematic processing (as in the *Rotaru* line of cases).

A more curious anomaly appears in the recent IACtHR decision in *CAJAR*, which concerned, inter alia, the surveillance and harassment of members of a human rights organisation (CAJAR) since the 1990s. In this judgment, the Court, when discussing information obtained from individuals, referred to a wide range of data, including public information, namely, information which is not inherently private and which has been/could be obtained from publicly accessible sources, such as the applicants' professional information. Yet, the Court made no distinction between the different categories of data at stake (see, e.g., para. 516), nor did it discuss whether this information – or which of it – falls within the scope of the right to private life. Later, the Court merely considered that the State's intelligence activities, including the acquisition and use of information 'including personal data', fell within (and constituted a breach of) individuals' rights, particularly the right to private life (e.g. paras. 520, 625). When addressing protections for information collected in the intelligence context, the Court referred more broadly to 'personal data', later clarifying that the term was understood in line with the OAS Principles (para. 572). More fundamentally, the Court declared the existence of an 'autonomous right' to informational self-determination under the ACHR, stating that 'the person is also free to exercise when and how much to reveal matters of their personal lives, which includes what type of information, including personal data, may be known by others' (para. 570). At face value, this suggests a complete alignment between the material scopes of privacy and data protection at the Inter-American level. However, the lack of elaboration leaves it uncertain whether this alignment reflects careful deliberation or merely a terminological/conceptual conflation. In any case, the alignment is complicated by the Court's joint analysis of privacy violations alongside other rights, such as freedom of expression. Indeed, the Court explicitly states that the right to informational self-determination – defined very broadly – manifests not only in the right to privacy (Art. 11 ACHR) but also in the rights to freedom of expression and judicial protection (Arts. 13 and 25) (para. 586).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

This makes it unclear which types of personal data fall within the scope of the right to private life and which are protected under other rights. This creates legal uncertainty about how future cases may be adjudicated if applicants rely solely on the right to private life, for example, because they cannot demonstrate downstream impacts on other rights.

Ultimately, the material scope of the right to privacy has been expanding under human rights jurisprudence. This expansion has occurred as IHRL bodies have become more willing to move beyond traditional and narrow conceptualisations of privacy (as captured in separation-based accounts; see Section 1.1). Increasingly, their decisions reflect a broader understanding of privacy, sometimes implicitly or explicitly echoing elements of control- and power-based perspectives on (information) privacy. This broadening has been made possible because IHRL bodies do not set out or endorse a single conceptualisation of privacy, but instead apply the right in a piecemeal manner in specific cases. However, this has also produced inconsistencies and a lack of clarity in the courts' reasoning. For instance, courts may overstate the 'privateness' of the information in question when they are in fact recognising an individual's right to control a broader range of information (e.g. the ECtHR in *Von Hannover*) or do the opposite, as in the IACtHR's *Fontevecchia*. They may also appear to move beyond a strict public–private dichotomy while still conditioning protection on whether the information is characterised as public or private (e.g. the ECtHR's *Rotaru* and similar approaches at the UN level). In these approaches, IHRL bodies seem to circle back to traditional conceptualisations of privacy even as they signal a greater willingness to broaden its scope. This is partly understandable, as IHRL bodies must demonstrate that the information in question is linked to individuals' 'private life' in accordance with the explicit wording of some IHRL treaties. However, it also overlooks the role of broader infrastructures in intruding on individuals' privacy interests. For the purposes of this section, this signifies a narrower material scope of (information) privacy compared with data protection. The latter covers any processing of personal data, regardless of the nature or context of the information involved.

3.2 Substantive Protections

Once the right to privacy is engaged (that is, where relevant information falls within its material scope), there is significant convergence between the protections offered under privacy and data protection frameworks. This convergence largely stems, again, from the broader conceptualisations of privacy that courts and treaty bodies often apply, even implicitly.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Many of the overlaps between the two regimes arise organically within privacy jurisprudence, reflecting the fact that data protection principles are, in large part, an expression or adaptation of existing human rights thinking to a technologically driven world. Under human rights law, once the right to privacy has been engaged in a particular case, the assessment of whether that right has been violated is undertaken in two stages: first, determining whether the right has been interfered with (the interference stage); and second, assessing whether that interference can be justified (the justification stage). The justification stage comprises three prongs: namely, whether interference is (i) provided by law, (ii) pursues a legitimate aim, and (iii) is proportionate. Many core data protection principles map onto each of these stages of human rights reasoning, though not always symmetrically or uniformly. The following analysis considers principles falling under the three main pillars of data protection frameworks – data subject participation, data controller obligations, and oversight – to examine the convergences and differences between the protections under data protection and those under privacy. It then offers final reflections on the relationship between (information) privacy and data protection in Section 3.3.

3.2.1 Data Subject Participation Pillar

Human rights jurisprudence also accommodates, to a large extent, the principles encompassed under the data subject participation pillar. For instance, human rights bodies often consider the absence of consent as a basis for finding an interference with the right to privacy (e.g. ECtHR *Malone* v. *UK* (1984), at para. 84 and UN HRC View on *Madhewoo* v. *Mauritius* (2021), para. 7.2). As most cases before these bodies concern processing operations carried out without the applicant's consent, it is difficult to speculate whether – and under what circumstances – they would also find an interference in cases where consent is present (Bygrave, 1998: 263). In situations where consent is absent, not through active refusal but in a more passive manner (i.e. where applicants are not asked), human rights bodies sometimes consider the applicant's reasonable expectations regarding how their information would be processed to indirectly determine the contours of their implied consent. For instance, in *MS* v. *Sweden* (1997), the ECtHR found an interference with the right to private life in relation to the sharing of the applicant's medical information with the Social Insurance Office, because '[i]t did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office' (para. 35). This approach towards

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

consent differs from the approach under (most) data protection frameworks, which emphasise that consent must be explicit and unambiguous. However, both data protection and privacy jurisprudence align to the extent that consent – albeit desirable – does not render processing lawful per se. Under human rights jurisprudence on privacy, the absence of consent is often reconsidered at the justification stage as a factor that calls for a more rigorous proportionality assessment (e.g. ECtHR, *S. and Marper* v. *UK* (2008), para. 104; see further Section 3.2.2 on proportionality). As under data protection law, the absence of individual control shifts the Court's focus to structures of architectural control: human rights bodies instead examine whether there are broader systemic safeguards that can nonetheless prevent undue interferences with individuals' information, such as adequate data security measures or oversight bodies (see further Sections 3.2.2 and 3.2.3).

The data subject rights are also largely reflected in human rights jurisprudence. Given the *modus operandi* of IHRL bodies in deciding cases in a piecemeal manner, these rights have not emerged as default or standalone rights under IHRL, but have instead been recognised through case-by-case assessments of applicants' requests concerning their personal information. There are two notable exceptions. First, GC No. 16 includes express references to the rights to rectification, to be informed, and to access and correct personal data, consistent with its function as an interpretative document setting out States' general obligations under the right to privacy. Importantly, the HRC explicitly ties these rights to the individual's right to 'control their files', which it evidently understands to be constitutive of (information) privacy (para. 10). The second exception is the *CAJAR* case, which extensively drew on the OAS Principles – including data subject rights – to unpack 'the right to information self-determination' under the ACHR (especially paras. 582–588). Separate from the question of whether these rights fall within the scope of the *right to privacy*, it is also worth noting that they were articulated in *obiter dicta*, as the Court acknowledged from the outset that the secret nature of surveillance necessarily precludes the individual's knowledge of the measure, and, by extension, their ability to participate in the processing of their data (para. 530).

Aside from these exceptions, data subject rights have emerged and been applied in a case-specific manner under IHRL jurisprudence for the above-mentioned reasons. For instance, in *Gaskin* v. *UK* (para. 37), the ECtHR found that the local authorities' rejection of the applicant's request to access his childhood records violated Art. 8. It held

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

that striking an appropriate balance between the applicant's right (to discover his 'basic identity') and public interest (to preserve the confidentiality of the staff's assessment) generated an (unmet) positive obligation to establish an independent supervisory mechanism 'through … [the UK's] … legal and administrative system' where access denials could be disputed (paras. 35, 38–39). In *Rotaru*, the ECtHR found that the inaccuracy of the information held on the applicant by the intelligence services (pertaining to his educational, political, and criminal records) together with the potential harm such information could cause to his reputation meant that the retention of his *fiche* and his inability to challenge the information therein constituted an interference with Art. 8, although the violation was primarily based on the vagueness of the surrounding legal framework. At the UN level, the HRC has recognised applicants' rights to correct and update their personal information. For instance, in *Coeriel and Aurik* v. *Netherlands* (1994), the HRC held that the right to privacy includes the right to choose and change one's name, as it 'constitutes an important component of one's identity' (para. 10.2). In that case, this extended to the authors' application to adopt a Hindu surname for religious reasons, which had been rejected. In *G* v. *Australia*, the HRC found a breach of the right to privacy where Australia's non-recognition of same-sex marriage prevented a transgender woman from changing her name and gender on her birth certificate unless she divorced after having undergone gender-affirming surgery after marriage. What is noteworthy about these cases is that IHRL bodies recognise privacy (here, referred to broadly as a multidimensional right, beyond its informational aspect) – as a right to lead a self-determined (autonomous) life. As a result, IHRL bodies have *also* recognised the rights of data subjects to control information more broadly about themselves, echoing control-based accounts of (information) privacy. This jurisprudence has, in effect, allowed individuals to exercise control over their information under privacy in ways similar to the control they could exercise through their data subject rights under data protection frameworks. Even at the IACtHR level, where the right to informational self-determination is grounded in a combination of rights, the Court specifically stresses that the '[r]ight to informational self-determination is an aspect of the protection of private life' under Art. 11 ACHR (para. 587), demonstrating that it, too, understands (information) privacy – at least in part – in control-based terms. However, it is significant that in internalising this control-based understanding of privacy, human rights jurisprudence holds that a breach does not arise from the mere rejection of applicants' claims, but from States'

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

failure to establish domestic oversight mechanisms allowing individuals to challenge and have such rejections reviewed. This reflects an understanding of (information) privacy not merely as a right enabling individual control but also as a right safeguarded by creating conditions for meaningful participation in the processing of personal information.

Three (additional) caveats are necessary regarding the apparent convergence between privacy and data protection in terms of data subject rights. The first, as explained, is that human rights bodies tend to uphold data subject rights on a case-by-case basis, unlike data protection frameworks, under which such rights exist as a general default. However, this difference should not be overstated: the different starting points under human rights and data protection might be insignificant if they actually yield the same practical results in specific cases, bearing in mind that data subject rights are also qualified and not upheld unconditionally. Second – and more importantly – is that when upholding data subject rights, human rights bodies often emphasise either the *nature* of the information or its *impact* on the applicants. This distinction stems from the limitations attached to the material scope of the right to privacy (Section 3.1). By proxy, it may narrow the circumstances in which such rights are available under the right to privacy, as compared with data protection. The latter generally grants these rights irrespective of the nature of the personal data or the consequences of its processing. This suggests that even when human rights bodies interpret the right to privacy in terms of informational self-determination – thereby granting individuals numerous data subject rights in specific cases – informational self-determination is understood more narrowly, being afforded to individuals only when the information relates to their private life and/or has a broader adverse impact on it.

Finally, there is a notable omission of certain rights falling under the data subject rights principle – such as the right to data portability and the right against ADM – from the jurisprudence on the right to privacy. As previously explained, these rights are not considered core aspects of data protection, largely because they are not recognised across all or most data protection frameworks. Nevertheless, their absence confirms Lynskey's observation that data protection goes beyond information privacy by granting individuals greater control over a broader range of personal data (see Section 3.1 on material scope) and by pursuing a wider array of rights. The first distinction – greater control – can be illustrated in particular with the right to data portability. The control-based interpretation of information privacy under human rights law, developed largely on a case-by-case

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

basis, could suggest that the current absence of a decision addressing the right to portability does not preclude its future recognition under the right to privacy if the circumstances of a case give rise to such a claim. Yet, as noted in Section 2.3, this right extends beyond privacy; given its close connection with economic and competition law, it is less likely to fall within – or be invoked under – the right to privacy. The second observation – that data protection safeguards a broader range of rights than privacy – is illustrated by the absence of a right against ADM in privacy jurisprudence, which, as discussed under Section 2.3, also reflects conceptual difficulties in accommodating this right within information privacy. In particular, none of the three understandings of (information) privacy offers an adequate account of how the act of making and applying algorithmic decisions itself constitutes an information privacy breach per se, as opposed to being a *consequence* of an (information) privacy breach[19] (although, to the extent that ADMs interfere with individuals' autonomy by steering them towards certain choices – often without their awareness – ADMs might be captured under other dimensions of privacy, such as *decisional* privacy).[20]

Indeed, the right against ADM can – and has been – comparatively better addressed under human rights jurisprudence on profiling. This jurisprudence engages predominantly the right to non-discrimination, rather than the right to privacy. For instance, *Basu* v. *Germany* (2022) and

[19] But see the emerging literature on group privacy (Taylor et al., 2017; see relatedly Vedder, 1999).

[20] The reasoning of the Hague District Court in the 2020 decision *SyRI*, concerning a human rights challenge to an ADM system used in the Netherlands for the purposes of preventing and combating social welfare fraud, provides an interesting example of a national court arguably sidestepping the difficult question of the extent to which Art. 8 ECHR can fully capture ADM-related challenges. Notably, the court examined the case under Art. 8 ECHR, which it interpreted in light of the data protection principles under EU law. In doing so, it merged the rights to privacy and data protection (even though they are provided as separate rights in the EU law, which it relied on for interpretation) by framing the latter as a procedural framework to elaborate the former. It considered ADM in the context of the right to privacy without explaining how the right can meaningfully extend to potentially discriminatory ADM; instead, the court skirted around the difficult question of the proper reach and scope by framing its assessment predominantly around the lack of transparency surrounding the ADM. Notably, the applicants did not raise a claim regarding the right to protection from discrimination taken together with the right to privacy; although they did raise an Art. 22 GDPR claim, which appears most relevant to this case, the court did not consider it necessary to assess that claim (see further discussion in Rachovitsa and Johann, 2022). While the court's approach arguably had the positive effect of combining different frameworks to deliver a human rights response in this instance without becoming mired in conceptual difficulties that might have muddled its reasoning, continued conceptual uncertainties have the practical effect of hampering the (consistent) development of privacy jurisprudence more broadly (see final observations, Section 3.3).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Lecraft v. *Spain* (2019) involved the ECtHR and HRC, respectively, tackling the identity checks performed on applicants of colour while they were travelling, whereas no such checks were undertaken on others present at the scene. In the former, the ECtHR held that singling out the applicant crossed the threshold of severity for the application of the right to privacy. This did not itself violate the right; the right, taken in conjunction with the protection from discrimination (Art. 14, ECHR), was violated *because* the State did not fulfil its positive obligation to adequately investigate the alleged discriminatory act. In other cases where protected characteristics were used exclusively or to a decisive extent as a basis for profiling to target individuals as criminal or antisocial and, thereby, their rights, the prohibition of discrimination was invoked in conjunction with other rights affected, such as the right to freedom of movement (e.g. the denial of border crossing to a Chechen applicant in ECtHR, *Timinishev* v. *Russia* (2005), para. 58) and the prohibition of cruel, inhuman, or degrading treatment (failure to prevent physical attacks on the Roma population in ECtHR, *Lingurar* v. *Romania* (2019), paras. 75–76), while the right to privacy was not raised at all (see also HRC's *Lecraft* v. *Spain* (2019), para. 7.2). It is worth noting that while concerns around (manual) profiling are thus better addressed under the right to non-discrimination, this right *also* falls short of fully addressing the issues raised by algorithmic profiling. This is because, unlike manual profiling, algorithmic profiling does not necessarily – or demonstrably – rely on protected characteristics, but instead operates based on a multitude of opaque factors, such as individuals being part of a group that frequents a particular online forum *and* regularly using a specific public transport route (Mittelstadt, 2017). The resulting profiles are often generated ad hoc and in real time, based on fluid and volatile criteria, making it virtually impossible to establish a causal connection between protected characteristics and differential treatment, as required under discrimination law. In that sense, the rights-based dimension of data protection arguably goes beyond the protections currently afforded under existing human rights frameworks. This, therefore, exemplifies an aspect of data protection that cannot be fully captured under information privacy or another right, such as protection from discrimination.

3.2.2 Data Controller Obligation Pillar

IHRL also demonstrates a level of overlap between the protections it offers and data controller obligations under data protection frameworks, although these overlaps are not always symmetrical or complete. Take, for instance, the principle of lawfulness. Under IHRL, any interference with the right to

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

privacy must be 'provided by law'. This requires that the interference has a basis in 'law', which can include a range of documents, such as domestic legislation, case-law, or guidelines (Gerards, 2023: 288–289). Differently, under data protection frameworks, lawfulness requires that processing occurs on a specific legal basis. This does not require, unlike under IHRL frameworks, that the relevant 'legal basis' has a formal source such as legislation; it can instead be grounded in bases such as data subjects' consent or their vital interests. However, it could be argued that domestic or regional data protection laws themselves constitute the 'law' under IHRL analysis, offering a framework that sets out the circumstances in which interferences arising from information processing are deemed permissible.

The requirement under IHRL that an interference be 'provided by law' also requires that the law meet two essential requirements of 'quality'. More specifically, the law should first be foreseeable, meaning that the domestic legal framework authorising interferences must be clear and not vague or open to multiple interpretations; and second, accessible, meaning that individuals must have an adequate indication of how the law would apply in different circumstances (see, e.g., ECtHR's *Malone* paras. 67 and 79; IACtHR's *Escher* v. *Brazil* (2009), para. 131; *CAJAR*, paras. 528–530; and HRC, *Pinkney* v. *Canada* (obiter dictum), para. 34). In effect, both criteria impose requirements on the State similar to those associated with transparency: where State information processing interferes with an individual's right to privacy (or 'private life'), the State should set out in 'law' key information about the processing operation and ensure that it is communicated in a clear and comprehensive manner. However, the nature of IHRL as a set of legal obligations binding on State Parties means that these requirements – while paralleling the transparency principle – do not apply as broadly as the transparency principle under data protection frameworks, which also bind private sector actors ('controllers') (Section 2.2). This reflects a broader distinction between the protections afforded under privacy and those under data protection.

Notably, these transparency-related requirements under IHRL apply even in national security contexts.[21] In national security contexts, human

[21] This also indicates a wider reach of IHRL protections in this specific context compared to data protection frameworks that provide exceptions for national security processing (Section 2.2). However, it is noteworthy that the right to privacy can also be qualified under IHRL frameworks on national security grounds, although such grounds do not provide for an exception to the right's application per se (unless the national security situation constitutes a public emergency allowing States to derogate from the right, e.g. Art. 15 ECHR).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

rights bodies have accepted that 'the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge' (*Malone* v. *UK* 1978, para. 55; see also *CAJAR*, para. 530). In these settings, IHRL bodies have held that foreseeability requirements cannot oblige States to 'enable[] … [individuals] … to foresee when authorities are likely to intercept his communications', as that would frustrate the purposes of surveillance (e.g. *Malone*, para. 67). This reinterpretation of the foreseeability requirement appears to require States to establish a form of generalised transparency in their surveillance operations by ensuring that the legal framework governing surveillance is clear and publicly accessible, thereby reducing the scope for arbitrary action. This mirrors the procedural dimension of fairness, which in turn serves as a tool for achieving a more substantively fair data processing system. The courts' emphasis on the risk of abuse generated by secret surveillance when articulating the foreseeability requirements appears to be underpinned by a power-based perspective on privacy. At the IACtHR, this concern with the power that surveillance confers on States is most forcefully expressed in the concurring opinion of Judge García Ramírez in *Escher*. While not part of the majority opinion, his view may be seen as an elaboration of some of the underlying concerns behind the majority's finding that the State's interception practices were unlawful for lacking the necessary clarity in law (as part of the foreseeability requirement) (paras. 147, 151). The judge's opinion, notably rich in vocabulary evoking authoritarianism, tyranny, and 'Big Brother', emphasised that privacy exists 'above and beyond the harm caused by the intruder', to protect against 'intolerable arbitrariness … [and] … abuse of [State] power' (e.g. paras. 5–7 and 111). This recognises that privacy interests in power-asymmetric contexts are not limited to protection from individual intrusion but also encompass broader concerns about a system in which the State can process and use information about individuals without limits (see further discussion under the oversight principle/pillar in Section 2). This power-focused perspective on (information) privacy is also reflected more broadly in human rights courts' substantive reasoning in secret surveillance cases, which has shifted from assessing individual breaches to examining the adequacy of safeguards (a shift also driven by certain practical and institutional constraints discussed below). In this context, it is striking that the broader impacts of surveillance on society and democracy are rarely properly or explicitly addressed in majority decisions (Hughes, 2015); instead, these considerations tend to emerge

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

in judges' separate opinions, possibly illustrating courts' reluctance to explicitly move beyond individualistic understandings of privacy, even when their substantive reasoning may point in that direction.

A relatively more symmetrical overlap between data protection and the right to privacy lies in the relationship between the data minimisation principle and the proportionality assessment under human rights law. Proportionality lies at the heart of the data minimisation principle, which requires that personal data be processed as minimally as possible in terms of quantity, quality, or duration. Some frameworks, such as the Ibero-American Standards (Art. 18), explicitly equate minimisation with proportionality. This overlap is also illustrated in IHRL jurisprudence. In *S. and Marper*, the ECtHR held that the police's retention of fingerprints, DNA profiles, and cellular samples of all accused individuals – regardless of acquittal or conviction – violated Art. 8, as it constituted 'blanket and indiscriminate' retention without independent review conducted based on predefined criteria, such as offence seriousness or prior arrests (para. 119). This echoes data minimisation and storage limitations requirements under data protection, which, as noted above, themselves give expression to the broader proportionality requirement found under IHRL. Similarly, in *Gaughran* v. *UK* (2020), the ECtHR found an Art. 8 breach because, although the police retained data only from convicted individuals, the retention policy failed to distinguish between minor and serious offences and did not assess whether continued retention was necessary (paras. 87–99). The ECtHR also found Art. 8 violations in cases where information about individuals was used for purposes different from – and incompatible with – those for which it was originally collected, reflecting the purpose-specification requirement. Relevant examples in the case-law include *M.S.* (sharing medical information with the social insurance office) and *Karabeyliođlu* v. Turkey (2016) (using intercepted communications collected for disciplinary proceedings in a criminal investigation). The reflection of these three prongs of the data minimisation principle – purpose specification, storage limitation, and data minimisation – under the right to privacy also mirrors the substantive dimension of fairness set out in data protection frameworks (which, again, itself reflects broader IHRL rules). This is because the three prongs included under the minimality principle serve to balance competing interests: by ensuring, first, that interference with the right to privacy pursues a 'legitimate aim'; and second, that this interference is strictly limited to what is necessary to achieve that aim.

Data security and sensitivity principles, as manifestations of the minimality principle, have also been considered under the proportionality

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

assessment in human rights jurisprudence. Given their interrelationships (Section 2.2), they have often been considered jointly. For instance, in *I* v. *Finland* (2008), which involved a nurse whose HIV-positive status became known to colleagues, the ECtHR found a violation of Art. 8 because the State had failed to implement a system to adequately secure sensitive information. The Court suggested that the hospital could have limited access to information concerning the applicant's infection to health professionals directly involved in her care or maintained an access log of all individuals who accessed her health data (para. 44). At the UN level, the sensitivity principle is not explicitly listed among the data protection principles in GC No. 16. However, this omission should not be considered conclusive, as the comment's brevity and the fact that it was drafted in the 1990s suggest that it cannot be understood as an exhaustive document (see, relatedly, Bygrave, 1998). Indeed, in its Views such as *Madhewoo* concerning a mandatory biometric ID programme involving uniquely identifying data such as fingerprints, the HRC explicitly emphasised the sensitivity of the data, which required the State to implement 'minimum safeguards' to ensure its protection (para. 7.6). The Committee found a violation of the right to privacy not because of the data collection itself but because Mauritius's decision to abandon centralised biometric data storage in response to public backlash had, *a contrario*, created new security vulnerabilities vis-à-vis hostile actors, increasing the risk of card theft and loss. These two cases from the ECtHR and the HRC reflect the three perspectives on information privacy simultaneously. First, a separation-based understanding is reflected in the fact that the privacy breach related to the actual (*I*) or potential (*Madhewoo*) third-party access to *intimate* information. Second, the ECtHR and HRC emphasised the non-consensual nature of the access, without which no privacy violation would have been found, reflecting that the concern was not with the disclosure of information per se but with the absence of individual control over that disclosure. Third, however, the violation of the right to privacy was not based on the disclosure itself, but on the State's failure to implement safeguards to prevent such access: in *I*, from colleagues; in *Madhewoo*, from hostile third parties. Both violations therefore stemmed not from direct State interference, but from State inaction. This shifts the focus to States' positive obligations to establish protective information-processing architectures, reflecting the power-based perspectives – or an expanded understanding of control-based accounts (including architectural control) – on information privacy. It is also worth noting that, while discrimination concerns were implicitly present in both cases – particularly in *I*, where

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

the applicant experienced differential treatment following the disclosure – the sensitivity and data security requirements were discussed squarely within the framework of the right to privacy, which remained the sole right substantively examined.

At the IACtHR level, the principles of data security and data sensitivity were expressly articulated in *CAJAR*, alongside several other core data protection principles set out in the OAS Principles, which the Court considered encompassed by the protections of the ACHR. While it is generally difficult to determine which data protection principle corresponds to which specific right – given that the Court in *CAJAR* assessed multiple rights jointly (e.g. privacy, honour, dignity, freedom of thought and expression, and children's rights) – the sensitivity principle appears to have been explicitly grounded in the right to privacy. The IACtHR emphasised that sensitive data warrants enhanced protections because they 'can be used to categorize a person and … develop[] personal profiles', thus clearly invoking privacy-based justifications rather than, say, anti-discrimination grounds (para. 554). This is despite the fact that both the right to privacy and protection from discrimination are discussed in equal terms under the sensitivity principle in the OAS Principles. In its earlier case-law, the IACtHR also addressed data security in cases involving the disclosure of information. In *Escher*, which concerned the interception and disclosure of telephone conversations of individuals associated with two social organisations (i.e. information which could only be obtained through intruding on private communications, thus information private by context), the Court found a violation of the right to privacy, inter alia, based on data security breaches. It held that it was highly probable that State agents had deliberately leaked the recordings to the press (para. 47). In this case, the breach of data security arose not from the State's omission, as in the former ECtHR and HRC cases, but from its affirmative act in disclosing information to others.

The final principle within the data controller obligations pillar is data accuracy. At the IACtHR level, this principle was cited among the OAS Principles that the Court in *CAJAR* considered encompassed by the ACHR, although the judgment suffers from the ambiguities noted above. As discussed, unlike other data controller obligations, which emerge more organically in privacy jurisprudence, data accuracy has a more uneasy relationship with privacy. While it can safeguard aspects of private life, it also functions more broadly as a tool protecting economic interests (e.g. efficient processing of personal data) and various rights and freedoms, such as protection against discrimination (e.g. by

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

ensuring that relevant and up-to-date information is used in decision-making) and the right to liberty and a fair trial (e.g. by ensuring arrests or trials are based on accurate information). This conceptual gap between data accuracy and privacy is reflected under IHRL jurisprudence. In particular, data accuracy has not been recognised as a general requirement within privacy jurisprudence, but rather indirectly, as a corollary of the right to rectification of personal data on a case-by-case basis. This recognition has occurred especially in cases where reputational interests are at stake, which are closely linked to the protection of one's 'private and family' life (e.g. *Khelili* v. *Switzerland* (2011), where the ECtHR recognised the applicant's right to rectify her registration in a police database as a prostitute on the basis of potential reputational harm). Accordingly, the existing jurisprudence suggests that IHRL does not confer a general right to seek the rectification of personal information as such (in the way that data protection frameworks do). Rather, the indirect recognition of data accuracy appears limited to situations where inaccurate information bears directly on an individual's private life or has tangible adverse consequences for it, understood in a relatively traditional and narrow sense (mirroring separation-based conceptions of privacy).

3.2.3 Oversight Pillar

Lastly, the oversight pillar entails, first, a set of risk-based obligations on data controllers to demonstrate compliance with data protection principles (accountability) and, second, the establishment of supervisory bodies to monitor such compliance (supervision). Starting with the latter, the HRC, which, unlike human rights courts, does have the tools to articulate States' general obligations under the ICCPR, has affirmed in its Concluding Observations the general requirement for States to establish independent bodies to oversee data processing operations as part of their obligations under the right to privacy (see, e.g., Concluding Observations on United States CCPR/C/USA/CO/5, para. 57 and Pakistan CCPR/C/PAK/CO/2, para. 45). However, in line with the general tendency of Concluding Observations to provide limited legal reasoning and mostly recommendations aimed at enhancing States parties' compliance with the ICCPR, these observations remain high-level and do not specify the qualities such oversight bodies should possess (Seibert-Fohr, 2017). Differently, the ECtHR and the IACtHR have reflected the requirement to establish oversight mechanisms in a case-specific manner, particularly in decisions concerning denials of individuals' claims to control their personal data. An exception to this case-specific approach arises

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

in a national security context, where these courts have emphasised the general requirement to establish oversight bodies tasked with supervising secret surveillance and set out its essential characteristics. This exception stems from two factors characterising national security settings: first, the secrecy that human rights bodies recognise as inherent to such environments; and second, the heightened risk of abuse that such secrecy enables (see, e.g., *Klass*, paras. 50, 55–56, and *CAJAR*, paras. 527). While the former limits individuals' ability to ascertain whether they have been subjected to surveillance, the latter underscores the importance of implementing adequate infrastructural safeguards to prevent abuses of power – one of which is the establishment of robust oversight mechanisms. According to these courts, such bodies must have broad jurisdiction, allowing anyone who suspects they have been subjected to surveillance to bring a claim, given the inherent difficulty of proving surveillance under secret regimes. Further, they should operate on a continuous basis, functioning ex ante to independently authorise interception orders and ex post to monitor surveillance practices throughout their life cycle. While it is not mandatory to assign this supervisory role to the judiciary, doing so may be preferable, as courts are more likely to meet key requirements, particularly independence (e.g. *Big Brother Watch* v. *UK*, paras. 351–359 and *CAJAR*, paras. 564–565). These conditions, although articulated specifically in national security contexts for the reasons outlined above, largely mirror the core requirements imposed on data protection authorities under the examined data protection frameworks generally.

This articulation of general accountability requirements represents an infrastructural turn, through which the courts have shifted focus from alleged individual harms to surveillance systems. Importantly, this turn also entails the incorporation of the accountability prong (i.e. risk-based obligations) into the right to privacy, albeit arguably in a manner that stretches both the right itself and human rights rules more broadly. This is evident in the way the ECtHR and IACtHR have (re)interpreted their rules on admissibility. Under the ECHR, for instance, only 'victims of a violation' may submit applications (Art. 34), and applicants must have 'suffered a significant disadvantage' (Art. 35). The ECtHR has interpreted these provisions as barring *actio popularis* claims, requiring individuals to be 'actually [adversely] affected' and prohibiting complaints based solely on the 'mere existence' of a law (e.g. *Klass*, para. 33). Similarly, at the Inter-American level, the Rules of Procedure (Rule 35(1)) require that victims in cases be identifiable. Both the Inter-American Commission (IACHR) and the IACtHR have confirmed that they will not consider

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

applications in *abstracto* (e.g. IACHR, *Montoya Gonzáles* v. *Costa Rica*, 1996). Despite these restrictions, both the European and Inter-American bodies have demonstrated notable flexibility in secret surveillance cases, where the fact of an individual's surveillance – and thus their victimhood – cannot be definitively established. For example, the ECtHR has acknowledged that 'under certain conditions', an applicant may claim victim status based on 'the mere existence of secret measures or legislation permitting secret measures, without having to allege that such measures were in fact applied to him' (*Klass*, para. 34). The Court later clarified that applicants may lodge claims either when 'remedies at the national level' are unavailable or when there exists a risk 'of secret surveillance measures being applied to [the applicant]' (*Kennedy* v. *UK*, 2010, para. 124). While this second condition appears to reintroduce the requirement of individual victimhood, the Court has interpreted it generously. In *Roman Zakharov* v. *Russia* (2015), for instance, it held that the relevant surveillance legislation 'directly affect[ed] all users of communication services by instating a system where any person can have his communications intercepted' (para. 170). In justifying this approach, the Court stressed that the mere existence of such legislation – even absent proof that it had been applied to the applicant – posed a 'threat of surveillance for all users of telecommunications services', alluding to the chilling effects of surveillance architectures (para. 178). Likewise, the IACtHR accepted the admissibility of secret surveillance claims in *CAJAR*, holding that the exception to Art. 35(2) of its Rules was fulfilled, referring, inter alia, to the covert nature of intelligence activities (paras. 94–95). This suggests that the Court applied reasoning similar to that of the ECtHR (whose jurisprudence it extensively relied on throughout the case), albeit in a less elaborate manner.

In doing so, both courts broaden their conceptualisation of privacy, focusing on the wider impact of surveillance at societal and structural levels, in line with a power-based perspective. Notably, this approach does not challenge the essentially individualistic nature of the right to privacy: the broader reading of admissibility rules is purposive, taking into account applicants' otherwise limited ability to challenge secret surveillance, as the victims are by definition unknown. However, this approach illustrates a degree of de-individualisation of privacy breaches. The courts diverge from the traditional human rights paradigm, which emphasises the applicant as 'an agent bearing specific characteristics' (Kosta, 2022: 213). Their focus is less on what has actually occurred vis-à-vis the individual applicant and more on what can take place under existing

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

secret surveillance infrastructures. The legal issue thus becomes 'not so much whether concrete harm has been done to a person in a concrete instance', but 'whether the law itself conforms to the principles of legality, legitimacy, and incorporates sufficient checks and balances to mitigate the risk of abuse of power' (Kosta, 2022: 216). The ECtHR's clarification that applicants' claims may also be based on the unavailability of remedies similarly underscores that the Court's fundamental concern lies in the Kafkaesque reality generated by secret surveillance. This marks a structural approach to the right to privacy and a turn towards regulating surveillance infrastructures ex ante. This mirrors the risk-based obligations imposed under data protection frameworks, which require data controllers to identify, anticipate, and mitigate the risks of data processing through designing data protection-compliant systems. Crucially, it is the power-based perspective on privacy that enables the integration of systemic and risk-oriented obligations into the human rights framework. This integration, and the infrastructural turn more generally, is desirable to some extent because it allows human rights bodies to address situations where breaches of information privacy – even in their most traditional forms, such as wiretapping individuals' communications – would otherwise have been difficult to assess due to State secrecy. At the same time, this turn results in broader regulation of information-processing structures, internalising tensions inherent to the power-based perspective on information privacy, whose implications are further discussed now.

3.3 Final Reflections

This section shows human rights bodies have interpreted the right to privacy – including, but also moving beyond, separation-based accounts to encompass control- and power-based approaches – has been instrumental in facilitating a significant degree of convergence with data protection principles. By incorporating relational, structural, and power-based dimensions into their interpretation of privacy, human rights bodies have reflected many core data protection principles in their jurisprudence on the right to privacy. Despite this, the overlap between privacy and data protection remains incomplete. Even as human rights bodies adopt bolder approaches – motivated by the protective goal of ensuring that human rights remain relevant to new digital technologies, for which the right to privacy often serves as the primary safeguard – there are limits to the extent to which these bodies have incorporated, or could justifiably incorporate, data protection elements into privacy jurisprudence. At the same time, conceptual uncertainties surrounding privacy and data

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

protection, and consequently their relationship, mean that these limits can often be identified only at a broad level and are difficult to implement with precision.

This has been a central challenge for human rights bodies, which have had to apply the right to privacy – despite its surrounding conceptual uncertainties – to the facts of specific cases. As a result, they have rendered decisions on the right to privacy in ways that are not always coherent or consistent. This is evident in the jurisprudence interpreting the material scope of the right to privacy. Courts have sought to broaden traditionally restrictive understandings of information privacy (as reflected in separation-based accounts), while simultaneously acknowledging that there are limits to what privacy can cover, without always clearly defining those limits. This is particularly apparent in IHRL bodies' treatment of 'public information', which is now recognised as falling within the scope of privacy *but* only when processed in 'systematic' ways, introducing an undefined criterion (which likely denotes *some* degree of extensiveness in processing). The IHRL approach to limiting the scope of privacy is understandable, given that such bodies can only consider claims relating to individuals' 'private life'. However, the private–public dichotomy it preserves can be overly restrictive. As explained, it may fail to extend protection to public information that is not systematically processed by the State at the time of the Court's assessment, but which may later be combined with other data – including by different actors – to generate more sensitive insights about individuals.

Similarly, with respect to substantive protections, IHRL jurisprudence indicates that the right to privacy struggles to encompass all principles found in data protection. At times, human rights bodies have simply refrained from incorporating certain principles – for instance, data accuracy, which has only been partially and indirectly recognised in privacy case-law. At other times, however, they have moved towards including additional principles, such as accountability obligations. Yet, such expansions risk drawing courts into the broader and more uncertain domain of information regulation, which risks further oscillations and inconsistencies in future privacy case-law, as partly arguably observed vis-à-vis material scope jurisprudence. Ultimately, conceptual ambiguities have, in some respects, had a positive effect by enabling courts to extend the scope of privacy to incorporate additional data protection principles. This has been particularly valuable in cases where applicants would otherwise be unable to challenge the use or application of certain technologies under data protection frameworks – either because no binding treaty or national law

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

exists or because such laws are inapplicable (for instance, due to national security exemptions). However, the by-product of this jurisprudence has been a catch-22 situation, further deepening the conceptual uncertainties surrounding the relationship between privacy and data protection.

All of this serves to buttress the overarching argument of this Element: that privacy and data protection overlap substantially, with the overlap becoming more extensive the broader privacy is understood, but that precisely delineating the contours of this overlap is extremely challenging, if not impossible. Nevertheless, it seems possible to suggest, based on the foregoing analysis, that data protection has an 'added value' in offering broader protections over a wider range of information compared with the right to privacy (see similarly Lynskey, 2014), *even if* the boundaries between privacy and data protection cannot be clearly delineated. There might even be an argument that a separate right to data protection is justified – or, where such a right does not exist, that it should be recognised in human rights treaties – because data protection safeguards rights that are not fully covered by pre-existing rights and freedoms. The recognition of a separate right could enable human rights bodies to interpret the right to privacy in more thoughtful ways, without the pressure of forcing important protections into the right to privacy as the 'next best' alternative available to them. That this right would inevitably overlap with other rights or freedoms is neither problematic nor novel; such overlaps are inherent in most human rights, and indeed applicants often invoke multiple rights jointly to demonstrate that an act or omission has breached their rights. What matters more is that a right to data protection would introduce protections that existing rights cannot fully encompass. That said, the introduction of such a right inevitably raises the question of which components of data protection frameworks can and should be incorporated into a human right to data protection. This Element does not seek to resolve that question but rather to highlight the need for greater clarity in the relationship between privacy and data protection – whether or not through recognising a separate right to data protection – while acknowledging the difficulties inherent in doing so.

4 Conclusion

Ultimately, therefore, rather than resolving the ambiguity in the relationship between privacy and data protection, this Element seeks to reflect on why this ambiguity exists and persists. It demonstrates that binary or ostensibly neat characterisations of this relationship – as either equivalent or contrasting notions – can only be sustained if one adopts a selective and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

narrow focus on specific dimensions of privacy or data protection. As the conceptual and legal analysis undertaken in this Element shows, the areas of overlap between the two expand and blur when more nuanced and holistic understandings of both concepts are adopted. All the same, this does not result in their complete convergence – most notably because data protection pursues a plurality of aims and contains protections, not all of which may be easily captured by the right to privacy or other rights, even as the boundaries between privacy and data protection remain difficult to delineate. The inherently multifaceted and evolving nature of both concepts generates and sustains ambiguity around their respective scopes and the interests they protect, which, in turn, obscures the ability to determine where one ends and the other begins. The introduction of a separate right to data protection to capture the additional protections offered under data protection frameworks in human rights law might be one possible means of easing the pressure on human rights courts and treaty bodies to fit an increasing number of data protection principles under the right to privacy. At the same time, such an approach would re-engage the challenge of determining which elements of data protection principles could be encompassed within such a right as suitable for inclusion within human rights frameworks.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Appendix

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978).

Asia-Pacific Economic Cooperation Privacy Framework (adopted 2015).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe) (Convention 108) (adopted on 28 June 1981). Updated by Modernized Convention on 18 May 2018.

Economic Community of West African States Supplementary Act A/SA.1/01/10 on Personal Data Protection within Ecowas (adopted on 16 February 2010).

European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953).

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980 and amended 11 July 2013).

International Convention on Civil and Political Rights (adopted 19 December 1966, entered into force 23 March 1976), 999 UNTS 171.

Organisation for American States, Updated Principles on Privacy and Personal Data Protection (originally adopted 2012 and updated 31 December 2001).

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data OJ L 119/1, ELI (adopted 27 April 2016) (replacing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31–50).

United Nations Guidelines for the regulation of computerized personal data files (adopted 21 July 1988).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

References

Abrusci, E., 2023. Factors Explaining Judicial Convergence and Fragmentation, in: *Judicial Convergence and Fragmentation in International Human Rights Law: The Regional Systems and the United Nations Human Rights Committee*. Cambridge University Press, pp. 95–243.

Allen, A. L., 2011. The Electronic Data Give-Away, in: *Unpopular Privacy: What Must We Hide?* Oxford University Press, pp. 156–172.

Allen, A. L., 2000. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. *Connecticut Law Review* 32, 861–875.

Altman, I., 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publishing Company.

Ausloos, J., 2020. *The Right to Erasure in EU Data Protection Law*, 1st ed. Oxford University Press.

Ausloos, J., Dewitte, P., 2018. Shattering One-way Mirrors – Data Subject Access Rights in Practice. *International Data Privacy Law* 8, 4–28.

Austin, L. M., 2014. Enough about Me: Why Privacy Is about Power, Not Consent (or Harm), in: Sarat, A. (Ed.), *A World without Privacy*. Cambridge University Press, pp. 131–189.

Ayalew, Y. E., 2022. Untrodden Paths towards the Right to Privacy in the Digital Era Under African Human Rights Law. *IDPL* 12, 16–32.

Basri, N., 2026. Regulating Surveillance during Occupation through Core Data Protection Principles. *The International Journal of Human Rights* 1–31. www.tandfonline.com/doi/citedby/10.1080/13642987.2025.2602134?scroll=top&needAccess=true

Basu v. *Germany*, App No. 215/19 (ECtHR, 18 October 2022).

Benn, S., 1984. Privacy, Freedom, and Respect for Persons, in: *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, pp. 223–244.

Bennett, C. J., 1992. Data Protection and Public Policy in Europe and the United States, in: *Regulating Privacy*. Cornell University Press, pp. 12–44.

BeVier, L. R., 1995. Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection. *William & Mary Bill of Rights Journal* 4, 455–506.

Bieker, F., 2022. *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law, Information Technology and Law Series*. T.M.C. Asser Press, The Hague.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Big Brother Watch v. *UK*, App Nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).

Bloustein, E. J., 1964. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review* 39, 962–1007.

Bosua, R., Clifford, D., Qian, J., Richardson, M., 2025. Data Rights in Transition, in: *Elements in Data Rights and Wrongs*. Cambridge University Press.

Bradford, A., 2023. Globalizing European Digital Rights through Regulatory Power, in: Bradford, A. (Ed.), *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

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

Bygrave, L. A., 2014. Core Principles of Data Privacy Law, in: *Data Privacy Law: An International Perspective*. Oxford University Press, pp. 145–167.

Bygrave, L. A., 2010. Privacy and Data Protection in an International Perspective Privacy and Data Protection. *Scandinavian Studies in Law* 56, 165.

Bygrave, L. A., 2002. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Kluwer Law International.

Bygrave, L. A., 2001. The Place of Privacy in Data Protection Law Forum: Valuing Privacy: Legal Protections and Exceptions. *University of New South Wales (UNSW) Law Journal* 24, 277–283.

Bygrave, L. A., 1998. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology* 6, 247–284.

Calo, R., 2011. The Boundaries of Privacy Harm Essay. *Indiana Law Journal* 86, 1131–1162.

Clifford, D., 2024. *Data Protection Law and Emotion*. Oxford University Press.

Clifford, D., 2022. The Data Protection Fairness Principle and the GDPR, in: *Oxford Encyclopedia of EU Law, Oxford Public International Law*. Oxford University Press.

Clifford, D., Ausloos, J., 2018. Data Protection and the Role of Fairness. *Yearbook of European Law* 37, 130–187.

Cobbe, J., 2026. A Relative Mess: Identifying Data Subjects in Multi-Party Processing. *Computer Law & Security Review* 62, 106362.

Coeriel and Aurik v. *the Netherlands*, HRC Communication No. 453/1991 (9 December 1994).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Cohen, J. E., 2019a. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Cohen, J. E., 2019b. Turning Privacy Inside Out. *Theoretical Inquiries in Law* 20, 1–31.

Cohen, J. E., 2012. What Privacy Is for Symposium: Privacy and Technology. *Harvard Law Review* 126, 1904–1933.

Cohen, J. E., 2008. Privacy, Visibility, Transparency, and Exposure Symposium: Surveillance. *University of Chicago Law Review* 75, 181–202.

Cohen, J. E., 2000. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review* 52, 1373–1373.

Concluding observations on the fourth periodic report of the United States of America (No. CCPR/C/USA/CO/5), 2014.

Cormack, A., 2016. Portability Right: A Data Protection Challenge – Regulatory Developments. Jisc Regulatory Developments. https://regulatorydevelopments.jiscinvolve.org/wp/2016/12/20/portability-right-a-data-protection-challenge/ (accessed 29 April 2025).

Dalla Corte, L., 2020. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection, in: Hallinan, D., Leenes, R., Gutwirth, S., De Hert, P. (Eds.), *Data Protection and Privacy*. Hart Publishing, pp. 27–58.

De Hert, P., Gutwirth, S., 2016. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in: Claes, E., Duff, A., Gutwirth, S. (Eds.), *Privacy and the Criminal Law*. Intersentia.

De Hert, P., Gutwirth, S., 2009. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in: Gutwirth, Serge, Poullet, Y., De Hert, Paul, de Terwangne, C., Nouwt, S. (Eds.), *Reinventing Data Protection?* Springer Netherlands, pp. 3–44.

Escher et al. v. *Brazil*, Judgment (Preliminary Objections, Merits, Reparations and Costs) IACtHR Series C No. 184 (6 July 2009).

Fontevecchia and D'Amico v. *Argentina*, (Merits, Reparations, and Costs) IACtHR Series C No. 37 (29 November 2011).

Foucault, M., 1991. *Discipline and Punish: The Birth of the Prison*. trans. Alan Sheridan. Penguin.

Fried, C., 1968. Privacy. *The Yale Law Journal* 77, 475–493. https://doi.org/10.2307/794941

G v. *Australia*, HRC Comm No. 2172/2012 (28 June 2017).

Gandy, O. H., 2016. *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Routledge.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Gaskin v. *UK*, App No. 10454/83 (ECtHR, 7 July 1989).

Gaughran v. *UK*, App No. 45245/15 (ECtHR, 13 February 2020).

Gerards, J., 2023. *General Principles of the European Convention on Human Rights*. Cambridge University Press.

Gerety, T., 1977. Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review* 12, 233–296.

Gerstein, R. S., 1978. Intimacy and Privacy. *Ethics* 89, 76–81.

Goffman, E., 1959. *The Presentation of Self in Everyday Life*. Doubleday Anchor.

González Fuster, G., 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series*. Springer International Publishing.

González Fuster, G., Gutwirth, S., 2013. Opening up Personal Data Protection: A Conceptual Controversy. *Computer Law & Security Review* 29, 531–539.

Greenleaf, G., 2014. Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. *Journal of Library and Information Science* 23, 4–49.

Gross, H., 1971. Privacy and Autonomy, in: *Privacy and Personality*. Routledge.

Herbecq and the Association 'Lingue des droits de l'homme' v. *Belgium*, App Nos. 32200/96 and 32201/96 (ECommHR, 14 January 1998).

Hijmans, H., 2016. *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU, Law, Governance and Technology Series*. Springer International Publishing.

Hildebrandt, M., 2015. *Smart Technologies and the End(s) of Law*. Edward Elgar Publishing.

HRC, 2017. Concluding observations on the initial report of Pakistan (No. CCPR/C/PAK/CO/2).

HRC, 2016. Concluding observations on the 7th periodic report of Colombia (No. CCPR/C/COL/CO/7).

Hughes, K., 2015. The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse, in: Roessler, B., Mokrosinska, D. (Eds.), *Social Dimensions of Privacy*. Cambridge University Press, pp. 225–243.

Hughes, K., 2012. A Behavioural Understanding of Privacy and Its Implications for Privacy Law. *Modern Law Review* 75, 806–836.

Hughes, K., 2009. Photographs in Public Places and Privacy Comment and Analysis. *Journal of Media Law* 1, 159–172.

I v. *Finland*, App No. 20511/03 (ECtHR, 17 July 2008).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Inness, J. C., 1996. *Privacy, Intimacy, and Isolation*. Oxford University Press.

Jančiūtė, L., 2017. EU Data Protection and 'Treaty-base Games': When Fundamental Rights are Wearing Market-making Clothes, in: Leenes, R., Brakel, R. van, Hert, P. D., Gutwirth, S. (Eds.), *Data Protection and Privacy: The Age of Intelligent Machines*. Hart Publishing, pp. 1–32.

Kaminski, M. E., 2022. The Case for Data Privacy Rights (Or 'Please, a Little Optimism').

Karabeyloglu v. *Turkey*, App No. 30083/10 (ECtHR, 7 June 2016).

Kennedy v. *United Kingdom*, App No. 26839/05, (ECtHR, 18 May 2010).

Khelili v. *Switzerland*, App No. 16188/07 (18 October 2011, ECtHR).

Kirby, M., 1999. Privacy Protection, a New Beginning: OECD Principles 20 Years on. Privacy Law and Policy Reporter.

Klass and Others v. *Germany*, (1979) 2 EHRR 214.

Koops, B.-J., Newell, B. C., Timan, T., Chokrevski, T., Gali, M., 2017. A Typology of Privacy. *Politica e Società* 3, 483–575.

Kosta, E., 2022. Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights. *Regulation & Governance* 16, 212–224.

Lazaro, C., Métayer, D. L., 2015. Control Over Personal Data: True Remedy or Fairy Tale? *SCRIPTed* 12, 3–34.

Lecraft v. Spain, HRC Communication No. 1493/2006 (17 August 2019).

Lingurar v. *Romania*, App No. 48474/14, (ECtHR, 16 April 2019).

Lynskey, O. (2014). Deconstructing Data Protection: The 'Added-Value' Of A Right to Data Protection in the Eu Legal Order. *International and Comparative Law Quarterly*, 63(3), 569–597.

Lynskey, O., 2015a. The Role of Individual Control over Personal Data in EU Data Protection Law, in: *The Foundations of EU Data Protection Law*. Oxford University Press, pp. 177–228.

Lynskey, O., 2015b. *Foundations of EU Data Protection Law, Oxford Studies in European Law*. Oxford University Press.

Lyon, D., 2007. *Surveillance Studies: An Overview*. Polity.

Madhewoo v. *Mauritius*, HRC Communication No. 3163/2018 (21 July 2021).

Malgieri, G., 2020. The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation. Presented at the Proceedings of FAT* '20, New York.

Malone v. *UK*, App No. 8691/79 (ECtHR, 2 August 1984).

Matsumi, H., Solove, D. J., 2024. The Prediction Society: AI and the Problems of Forecasting the Future. *University of Illinois Law Review* 1, 1–62.

Mayer-Schönberger, V., 1997. Generational Development of Data Protection in Europe, in: Agre, P. E., Rotenberg, M. (Eds.), *Technology and Privacy: The New Landscape*MIT Press, pp. 219–241.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Members of the Lawyers' Collective Corporation 'José Alvear Restrepo' v. *Colombia ('CAJAR')*, IACtHR (18 October 2023).

Miller, A. R., 1971. *Assault on Privacy: Computers, Data Banks and Dossiers*. University of Michigan Press.

Mittelstadt, B., 2017. From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology* 30, 475–494.

Montoya González v. *Costa Rica*, n.d., (Admissibility) IACHR OEA/Ser.L/V/II.95 Doc. 7OEA/Ser.L/V/II.95 Doc.7 (16 October 1996).

Moreham, N. A., 2008. Why Is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort, in: Finn, J., Todd, S. (Eds.), *Law Liberty, Legislation: Essays in Honour of Joh Burrows QC, Victoria University of Wellington Legal Research Paper No. 113/2015*. Social Science Research Network, pp. 231–247.

NCJM et al. and FNV v. *The State of the Netherlands ('SyRI')*, District Court of the Hague, 6 March 2020, ECLI:NL:RBDHA:2020:865, n.d.

Niemitz v. *Germany*, (1992) 16 EHRR 97.

Nippert-Eng, C. E., 2010. *Islands of Privacy: Selective Concealment and Disclosure in Everyday Life*. University of Chicago Press.

Nissenbaum, H. F., 1998. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy* 17, 559–596.

Nissenbaum, H. F., 1997. Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior* 7, 207–219.

Nissenbaum, H. F., 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

Nolan, K. A., 2023. The Individual in EU Data Protection Law (Thesis). LSE.

OECD, 2023. Explanatory Memorandum of the OECD Privacy Guidelines, OECD Digital Economy Papers.

O'Hara, K., 2023. *The Seven Veils of Privacy: How Our Debates About Privacy Conceal Its Nature*. Manchester University Press.

OHCHR, 2022. The right to privacy in the digital age (A/HRC/51/17).

Orji, U. J., 2017. Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act. *International Data Privacy Law* 7, 179–189.

Parent, W. A., 1983. Privacy, Morality, and the Law. *Philosophy & Public Affairs* 12, 269–288.

Peck v. *the United Kingdom*, App No. 44647/98 (ECtHR, 1 March 2003).

PG and JH, App No. 44787/98 (ECtHR, 25 September 2001).

Pinkney v. *Canada*, HRC Communication No. 27/1878 (2 April 1980).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Quelle, C., 2017. Not Just User Control in the General Data Protection Regulation. On the Problems with Choice and Paternalism, and on the Point of Data Protection.

Rachels, J., 1975. Why Privacy Is Important. *Philosophy & Public Affairs* 4, 323–333.

Rachovitsa, A., Johann, N., 2022. The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case. *Human Rights Law Review* 22.

Reiman, J. H., 1976. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs* 6, 26–44.

Richards, N. M., 2022. *Why Privacy Matters*. Oxford University Press.

Richards, N. M., 2013. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford University Press.

Richards, N. M., 2008. Intellectual Privacy. *Texas Law Review* 87, 387–446.

Richards, N. M., King, J. H., 2013. Three Paradoxes of Big Data. *Stanford Law Review* 66, 41–46.

Richardson, M., 2017. *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea, Cambridge Intellectual Property and Information Law*. Cambridge University Press.

Rodotà, S., 2009. Data Protection as a Fundamental Right, in: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (Eds.), *Reinventing Data Protection?* Springer Netherlands, pp. 77–82.

Roessler, B., 2018. *The Value of Privacy*. John Wiley & Sons.

Rotaru v. *Romania*, App No. 28341/95 (ECtHR, 4 May 2000).

Rouvroy, A., 2008. Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. Studies in Ethics, Law, and Technology 2.

Rubenfeld, J., 1989. The Right of Privacy. *Harvard Law Review* 102, 737–807.

S and Marper v. *UK*, App Nos. 30562/04 and 30566/04 (ECtH, 4 December 2008).

Schoeman, F., 1984. Privacy: Philosophical Dimensions of the Literature, in: Schoeman, F. D. (Ed.), *Philosophical Dimensions of Privacy*. Cambridge University Press, pp. 1–33.

Schwartz, G. T., 1990. Explaining and Justifying a Limited Tort of False Light Invasion of Privacy Symposium: The Right to Privacy One Hundred Years Later. *Case Western Reserve Law Review* 41, 885–920.

Schwartz, P. M., 1999. Internet Privacy and the State Commentary. *Connecticut Law Review* 32, 815–860.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Seibert-Fohr, A., 2017. The Human Rights Committee – Legacy and Promise, in: *International Human Rights: Human Rights Institutions, Tribunals and Courts – Legacy and Promise*. Springer. https://link.springer.com/referencework/10.1007/978-981-10-5206-4

Sitaropoulos, N., 2015. States are Bound to Consider the UN Human Rights Committee's Views in Good Faith | OHRH. Oxford Human Rights Hub. https://ohrh.law.ox.ac.uk/states-are-bound-to-consider-the-un-human-rights-committees-views-in-good-faith/ (accessed 9 January 2025).

Solove, D. J., 2025. *On Privacy and Technology*. Oxford University Press.

Solove, D. J., 2022. The Limitations of Privacy Rights. *Notre Dame Law Review* 98, 975–1036.

Solove, D. J., 2021. The Myth of the Privacy Paradox. *George Washington Law Review* 89, 1–51.

Solove, D. J., 2013. Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126, 1880–1903.

Solove, D. J., 2008. *Understanding Privacy*. Harvard University Press

Solove, D. J., 2007. I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review* 44, 745–772.

Solove, D. J., 2004. Architecture and the Protection of Privacy, in: *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.

Solove, D. J., 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review* 53, 1393–1462.

Taylor, L., Floridi, L., Van Der Sloot, B. (Eds.), 2017. *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing.

Timishev v. *Russia*, App Nos. 55762/00 and 55974/00 (ECtHR, 13 December 2005).

Tzanou, M., 2013. Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not so New Right. *International Data Privacy Law* 3, 88–99.

van der Sloot, B., 2020. Regulating Non-personal Data in the Age of Big Data, in: Tzanou, M. (Ed.), *Health Data Privacy under the GDPR*. Routledge.

van der Sloot, B., 2017. Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR, in: Taylor, L., Floridi, L., van der Sloot, B. (Eds.), *Group Privacy: New Challenges of Data Technologies, Philosophical Studies Series*. Springer International Publishing, pp. 197–224.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Vedder, A., 1999. KDD: The Challenge to Individualism. *Ethics and Information Technology* 1, 275–281.

Véliz, C., 2024. *The Ethics of Privacy and Surveillance*. Oxford University Press.

Véliz, C., 2020. *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. Bantam Press.

Viljoen, S., 2021. A Relational Theory of Data Governance Feature. *Yale Law Journal* 131, 573–654.

Warren, S. D., Brandeis, L. D., 1890. Right to Privacy. *Harvard Law Review* 4, 193–220.

Westin, A. F., 1967. *Privacy and Freedom*, 1st ed. Atheneum.

Zakharov v. *Russia*, ECtHR, 4 December 2015.

Zuboff, S., 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Acknowledgment

I am very grateful to the editors of the Elements, especially Damian Clifford and Megan Richardson for their their helpful comments and suggestions. I also wish to extend my sincere thanks to Michael Veale and Kimberley Trapp for their feedback on the earlier drafts of this piece.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Cambridge Elements

Data Rights and Wrongs

Damian Clifford

London School of Economics

Damian Clifford is an Assistant Professor at the London School of Economics and Political Science. Previously a Senior Lecturer and Postdoctoral Research Fellow at the Australian National University, and FWO Aspirant Fellow at KU Leuven's Centre for IT and IP Law (CiTiP), his research focuses on data protection, privacy and technology regulation, and he has published across these fields. His recent books are *Data Rights and Private Law* (ed with Jeannie Marie Paterson and Kwan Ho Lau, 2023); *Data Protection Law and Emotions* (2024); and *Data Rights in Transition* (with Rachelle Bosua, Jing Qian and Megan Richardson, 2025).

Jeannie Marie Paterson

University of Melbourne

Jeannie Marie Paterson is Director of the Centre for AI and Digital Ethics at the University of Melbourne and a Professor of Law at the Melbourne Law School. Her research focuses on themes of support for vulnerable consumers; the regulation of new technologies in consumer and financial markets; and regulatory design for protecting consumer rights and promoting safe, fair and accountable technologies. Her recent books include *Misleading Silence* (ed with Elise Bant, 2020); and *Data Rights and Private Law* (ed with Damian Clifford and Kwan Ho Lau, 2023).

Editorial Board

Mark Andrejevic, *Professor, Communications & Media Studies, Monash Data Futures Institute*

Sara Bannerman, *Professor, McMaster University, and Canada Research Chair in Communication Policy & Governance*

Rachelle Bosua, *Senior Lecturer, Deakin University; Honorary Senior Fellow, School of Computing and Information Systems, the University of Melbourne*

Jake Goldenfein, *Senior Lecturer, Melbourne Law School, the University of Melbourne*

Claes Granmar, *Associate Professor, Faculty of Law, Stockholm University*

Sonia Katyal, *Associate Dean of Faculty Development & Research, Co-Director Berkeley Center for Law & Technology, Roger J Traynor Distinguished Professor of Law, UC Berkeley*

Andrew Kenyon, *Professor of Law, Melbourne Law School, the University of Melbourne*

Orla Lynskey, *Professor of Law and Technology, University College London*

Frank Pasquale, *Professor of Law, Cornell Tech and Cornell Law School, New York*

Julia Powles, *Executive Director of the UCLA Institute for Technology, Law, and Policy; Professor of Practice; Tech Policy Lead, UCLA DataX*

Trisha Ray, *Associate Director and Resident Fellow, GeoTech Center, Atlantic Council*

Megan Richardson, *Honorary Professor, Melbourne Law School, the University of Melbourne*

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Julian Thomas, *Director of the ARC Centre of Excellence for Automated Decision-Making and Society; Distinguished Professor, School of Media and Communication, RMIT University*
Peggy Valcke, *Professor of Law & Technology and Vice-Dean of Research, Faculty of Law & Criminology, KU Leuven*
Normann Witzleb, *Associate Professor of Law, Chinese University of Hong Kong*

About the Series

This Cambridge Elements series provides a home for fresh arguments about data rights and wrongs along with legal, ethical and other responses. We encourage new ways of thinking about data as enmeshed within social, institutional and technical relations.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085

Cambridge Elements

Data Rights and Wrongs

Elements in the Series

Data Rights in Transition
Rachelle Bosua, Damian Clifford, Jing Qian, and Megan Richardson

Data Access and AI Explainability
Frank Pasquale

Addressing Misinformation and Disinformation
James Meese and Corinne Tan

AI Mental Health Support and the Case for Distributed Networked Regulation
Jeannie Marie Paterson

Revisiting the Relationship between Privacy and Data Protection
Nahide Basri

A full series listing is available at: www.cambridge.org/EDRW

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 15:34:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009854085