Appears in *Research Handbook on Law and Technology* (p. 214-221)
Edited by Bartosz Brożek, Olia Kanevskaia & Przemysław Pałka
Elgar, 2023

Privacy at a Crossroads*

ARTUR PERICLES L. MONTEIRO
Yale Jackson School of Global Affairs & Yale Law School

The right to privacy is at a crossroads. It was once the subject of intense theoretical disputations; a pragmatic turn thrust it into the spotlight of the most salient disputes about the regulation of technology, surveillance, and informational capitalism. Yet at the same time that privacy law's reach has become vast, there is no agreement on whether and how it can actually provide the answers that society expects to the most pressing questions of our days. If anything, the agreement increasingly seems to be that it can't. The most exciting paths now being chartered instead are perhaps best read as moving "beyond privacy" and towards "data governance". This chapter tracks this trajectory of the right to privacy, focusing on informational privacy. It raises questions we might want to answer before abandoning it as an old toy and discusses potential problems and limitations for data governance.

*I am grateful to Przemek Pałka and Olia Kanevskaia Whitaker for generous feedback and to Marina Federico for insightful discussion and literature recommendations.

The right to privacy is at a crossroads. It was once the subject of intense theoretical disputations around not only its value and delineation (see, *e.g.*, the essays compiled at Schoeman, 1984a), but also its very existence (*e.g.* Thomson, 1975) as a "distinct and coherent" right (Schoeman, 1984b).[1] A pragmatic turn (Solove, 2002, 2008) thrust it into the spotlight of the most salient disputes about the regulation of technology, surveillance, and informational capitalism. Yet at the same time that privacy law's reach has become so broad that it is often (and not approvingly) referred to as the "law of everything" (Purtova, 2018), there is no agreement in how it can actually provide the answers that society expects to the most pressing questions of our days. If anything, the agreement increasingly seems to be that it can't. The most exciting paths now being chartered instead is perhaps best read as moving "beyond privacy" (Pałka, 2020) — and towards "data governance" (Viljoen, 2021).

This chapter tracks this trajectory of the right to privacy, focusing on informational privacy. It outlines its past of intense theoretical disputes and calls attention to the shift in the conceptualization of privacy embodied by the pragmatic turn. It also discusses the latest developments in the transition from privacy law to data governance. It raises questions about the paths not taken for privacy law, which we might want to answer before abandoning it as an old toy. And it discusses potential problems and limitations for data governance.

Before we proceed, a note on terminology. While the discussion here adopts "the right to privacy" unqualifiedly, it speaks to what is often termed informational privacy (*e.g.* Roessler, 2005, pp. 110–141), or information privacy (*e.g.* Richards, 2006). It does not take up other aspects of the right to privacy, such as decisional privacy (Roessler, 2005, p. 79), alternatively constitutional privacy (Tugendhat, 2017, p. 132), under which questions on reproductive rights (e.g. abortion and access to contraceptives), among others, are often discussed (see Marmor, 2015, pp. 23–25 for an objection to the decisional dimension of privacy). Informational privacy, taken as "the dimension of privacy that concerns information or data about a person" (Roessler, 2017, p. 200), is often seen as synonymous with data protection (*e.g.* Flaherty, 1991, p. 832). Further, there is debate about whether data protection is a synonym for (this dimension of) privacy, or is distinct from it, is in the service of privacy only, or other rights and interests as well (see, *e.g.* Gellert & Gutwirth, 2013). And of course positive law can regulate data protection in a particular manner, attaching to it requirements, procedures, effects and institutions that do not attach to the right to privacy more generally (Kokott & Sobotta, 2013). I do not mean to take a view regarding this debate. My goal is to briefly examine a shift in thinking about these issues, under whatever heading they are cabined.

214 ↑
↓ 215

I. PRIVACY BEFORE THE TURN

Legal scholars writing about the right to privacy cannot seem to resist the urge to trace it to Samuel Warren and Louis Brandeis's 1890 *Harvard Law Review* article "The right to privacy" (Warren & Brandeis, 1890; see, *e.g.*, Citron, 2022, pp. xii–xiii; Regan, 1995, pp. 14–15; Richards, 2022, p. 17; Solove, 2008, p. 1; Solow-Niederman, 2022, p. 368; Waldman, 2018, p. 11). There is perhaps good reason for this. Warren and Brandeis were responding to the challenges emerging technology and business models — "[r]ecent inventions and business methods"

[1] Note that this theoretical question is not resolved by the fact that privacy is codified, *e.g.*, under the International Covenant on Civil and Political Rights, regional human rights systems, or national constitutions. Thomson's objection was that "every right in the right to privacy cluster is also in some other right cluster" (1975, p. 313). The codification of a right to privacy does not negate that claim, both because bills of rights also have a symbolic meaning and because it would still need to be shown that Thomson was wrong that a privacy violation can occur without a violation of another, non-derivative right. See, for instance, Scanlon (1975).

(Warren & Brandeis, 1890, p. 195) — posed to "the protection of the person". That might well serve as a description of what drives so much of the discussion about privacy today. Their argument was that a right to privacy should be recognized as part of "the more general right of the individual to be let alone" and the principle of "inviolate personality" (Warren & Brandeis, 1890, p. 205) which law, particularly tort law, undertakes to protect, regardless of "the interposition of the legislature" (Warren & Brandeis, 1890, p. 195).

There is debate about the extent to which Warren and Brandeis amounted to a revolution in thinking about privacy, and the extent to which they were successful. Neil Richards and Daniel Solove argue that they "did not write on a nearly blank slate" (Richards & Solove, 2007, p. 145) and rather deliberately took U.S. thinking on privacy on a divergent path from the English roots of confidentiality, which the famous 1890 article deemphasizes. James Whitman contends that the article ought to be seen as "an unsuccessful continental transplant" (2004, p. 1204) given how much it drew on German personality rights and French case law, noting it got a "cold reception" (2004, p. 1208). Meghan Richardson follows the trail from Rudolf von Jhering to classic liberalism and hypothesizes that, "through Warren and Brandeis, the ideas of earlier thinkers such as Bentham, Mill and von Jhering were extended further in ways that their originators might not have contemplated, but might eventually have approved" (Richardson, 2017, p. 9). The contribution she credits the U.S. duo with "popularizing" the right to privacy because of how they framed snapshot photography as impacting the average person, whereas it was "earlier largely treated as a bourgeois right" (Richardson, 2017, p. 9).

What matters to the discussion in this chapter is how the Warren–Brandeis article came to grasps with the right to privacy. Whatever its intellectual contribution or immediate impact on adjudication might have been, "The right to privacy" is characteristic of a mode of thinking about privacy that had staying influence. In 1960, William Prosser identified four separate torts that had been adopted by courts in the U.S. "by the use of a single word supplied by Warren and Brandeis" (Prosser, 1960, p. 422). To him, these torts represented "four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common" (Prosser, 1960, p. 389). He was challenged by Edward Bloustein (1964), who argued not only were the privacy torts tied by a common thread, but also that it extended to the regulation of government interferences under the Fourth Amendment to the U.S. Constitution— and that missing that thread jeopardized the development of the law of privacy, including for the tort remedies available. 215 ↑

Prosser was the reporter for the *Restatement (Second) of Torts*, and his view prevailed at ↓ 216 least to when it comes to the classification of the privacy torts (Schwartz & Peifer, 2010, pp. 1938–1939). That, of course, doesn't preempt conceptual articulation of the right to privacy. In fact, up to the 1990s, scholarship was marked by energetic arguments about the right to privacy, its existence as a standalone right, its value and its legal specification. Texts such as James Rachels (1975), Ruth Gavison (1984), Stanley Benn (1984), Judith Jarvis Thomson (1975), and Jeffrey Reiman (1976) debated what privacy means, what is its justification, and how the law should recognize it. These works remain widely cited today, including in highly influential work (Hadjimatheou, 2017; *e.g.* Koops et al., 2017; Richards & Hartzog, 2017; Roessler, 2005; Waldman, 2018). But they typically figure as relics of another era, a mode of thinking about privacy that has been left behind.

II. THE PRAGMATIC TURN

Indeed, the dominant thinking about privacy today stands in contrast to those texts. A perfect summary is provocatively provided by Woodrow Hartzog: "What is privacy? That's the wrong question" (Hartzog, 2021). Hartzog notes that Daniel Solove "has been extraordinarily influen-

tial for scholars, policymakers, and practitioners" (2021, p. 1680) and can take considerable credit for that now prevailing stance, which sees "chaos and futility [in] competing conceptualizations of privacy" (2021, p. 1679). Solove has been influential in his push for a pragmatic turn. To Hartzog, this turn means that:

> Instead of squabbling over the binary boundaries of privacy, people who understand privacy as more of a vague umbrella term can leave the line-drawing question for another day and get to work identifying problems created by specific conduct, articulating the values implicated by those problems, and crafting solutions to the problems that serve those values (Hartzog, 2021, p. 1681).

Whether Solove thinks conceptualizing privacy is not a priority but best left "for another day" (as Hartzog put it) or deems it "a quixotic search" (Calo, 2011, p. 1140) that should be dropped entirely is perhaps an open question. Regardless, Solove clearly positions his work in contrast with the earlier concerns in privacy thinking. In fact, not only that, he blames that mode of privacy thinking for the failures he diagnoses in addressing concrete problems: "The difficulty in articulating what privacy is and why it is important has often made privacy law ineffective and blind to the larger purposes for which it must serve" (Solove, 2002, p. 1090). Solove's theory is instead oriented towards "attempting to solve certain problems" (Solove, 2002, p. 1129). This is the reason why he catalogs 16 types of "privacy problems", or "privacy violations", and emphasizes the different components that go into responding to each of them (Solove, 2006).

It would be a mistake, however, to see this turn to just be about a focus on policy and having privacy get results. The pragmatic turn goes further than just setting aside the question of whether there is an overarching value in different manifestations of privacy problems. Solove is clear that "there is no overarching value of privacy" (2002, p. 1145). He also rejects a non-consequentialist account for the value of privacy (Solove, 2002, pp. 1144–1145). Here Solove's objection is not practical but about meta-ethics. He does not seek to refute the idea that privacy can have intrinsic value; his contrary position is premised on the idea that arguing about intrinsic value does not go beyond describing it as a "mere taste", such as a preference for vanilla ice cream (Solove, 2008, p. 84). 216↑

While not necessarily committed to a normative position on the value of privacy (or even ↓217 to grounding regulation on privacy: Gellert & Gutwirth, 2013; Kokott & Sobotta, 2013) data protection regimes such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are in agreement with the motivation behind the pragmatic turn in that its operation does not hinge on identifying what should be protected as private. Any data about a person attracts data protection legislation,[2] triggering an extensive list of record-keeping and other compliance mechanisms. While "privacy may hold much emotive and symbolic appeal" (Bennett, 1992, p. 13), data protection avoids what pragmatists see as the hopelessly subjective task of sorting through what should or should not count as covered (Bieker, 2022, pp. 179, 259). That shouldn't be overstated: value judgments can still be decisive in assessing whether, for instance, legitimate interests for data processing exist.[3] But the undeniable point is that data protection runs from another starting point — so much so that many have insisted that the latter has outgrown it and has as a separate life (See,

[2] Different regimes have their own delineations on the concept of personal data and personally identifiable information. This is a relevant factor for comparing their scope, but one that has no impact on their categorization as creatures of the pragmatic turn.

[3] It is noteworthy that under the GDPR adopts the language of "reasonable expectations" as a factor for determining the legality of data processing on the basis of legitimate interests. See Recital 47. Also see the opinion of the Article 29 Data Protection Working Party on legitimate interests (2014). While that opinion

e.g., Gellert & Gutwirth, 2013). In practice, this makes data protection so ambitious that its scope can extend to virtually any activity — it becomes "the law of everything" (Purtova, 2018). That is true of comprehensive legislation such as the GDPR and other legislation fashioned after it and, to a lesser extent, regimes like the CCPA.[4].

III. DATA GOVERNANCE AND THE FUTURE OF PRIVACY

The pragmatic turn extricated privacy from conceptual paralysis. The right to privacy gained ground with data protection legislation, not just in the E. U., but globally, including in several U.S. states. Yet this new ground gained after the turn has come at a cost. Joris van Hoboken has described it in terms of a *privacy disconnect*: "a divide between the demands for [the] legitimacy [of pervasive data processing] and what current privacy governance offers in practice" (Hoboken, 2019, p. 256).

That is, while data protection is expected to respond to the most dramatic questions facing society in terms of informational capitalism and widespread surveillance, this legislation has been made a victim of its own success — and can't deliver on its promises. The pragmatic turn made it operative (impactful, if not effective) to an extent that privacy law never was. Yet the complicated operation of the data protection machine does not provide answers directly. It relies on a proceduralized model that largely does not contain definitive, substantive positions (Gutwirth & Hert, 2006), and so can plausibly be articulated as legitimizing a sweep of data processing activities. This means that before enforcement action is taken — and survives judicial review — business practices which most see as objectionable and in contradiction with data protection legislation are speeding ahead in full steam, coated in the veneer of legality gifted by proceduralized privacy law. 217 ↑ ↓ 218

Even if that could be overcome, data protection regimes are faced with more fundamental objections, aimed at the role of consent (N. Richards & Hartzog, 2019; Solove, 2013). Notice and consent, or choice, is described as unfeasible in practice, not least because of informational overload. It is canonical in scholarship that consent-based models are obsolete and doomed to fail. Yet, at the risk of heresy, perhaps the demise of consent might have been announced prematurely: Apple's privacy changes (Kollnig et al., 2022) were leveraged by swathes of users, and albeit imperfect seem consequential enough that Mark Zuckerberg blamed them for at least part of Meta's gloomy prospects (Conger & Chen, 2022). It is not clear that data protection law wouldn't be able to overcome the practical problems surrounding consent with modifications that preserve the edifice while making consent more meaningful.[5]

One potential route would be to establish a baseline, deviation from which would require consent. This might be achieved with default rules regarding data practices to which consent might be given, thus creating an incentive for abiding by such default rules at the same time that departure from them would only then merit attention from the data subject. Operating systems could be set up on the basis of those default rules or other user preferences, thereby

was issued under the Data Protection Directive (Directive 95/46/EC), the European Data Protection Board has relied on it to discuss lawful grounds for data processing under the GDPR. See, e.g., the guidelines on consent (2020).

4 Although not as wide as the GDPR in scope, the CCPA still goes much further than prior, sectoral, legislation in the U.S. See Chander et al. (2021, p. 1759), which contrasts the "data protection" language of the GDPR to the information privacy of U.S. legislation.

5 Making consent more meaningful, of course, does not address objections such as Pałka's (2020, p. 630), who notes that "given the potential for externalities, and the fact that one person's disclosure imposes data-driven costs on other people, individuals should not be the only decision-makers." I don't disagree; indeed, consent is not the sole criterion for legitimate data processing, be it under the GDPR or under HIPAA. I would note that is a different issue, which does not undermine the *feasibility* of consent mechanisms.

granting consent automatically without the user being asked each time, but only for processing that doesn't match their preferences. Another potential approach would be enacting more detailed, sectoral regulation, such as what the US's HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule does for patient data disclosures to family members, for instance.[6] The point here is that consent doesn't have to look like it does right now, with cookie banners galore.

A second challenge to consent as the centerpiece of data protection blames it for its insignificance. Consent is rendered meaningless given the data "tyranny of the minority", that is, the fact that often "the volunteered information of the few can unlock the same information about the many".(Barocas & Nissenbaum, 2014, p. 61) That is, if consent is the legitimation for data processing, then individuals are deprived of their autonomy when inferences about them can be made on the basis of data collected from a smaller number who have consented. This time, the challenge seems to prove too much: while it is true that information about a population can be obtained without agreement from the majority of the population, that holds for "big data" as it does for statistics, opinion polls, and focus groups. Why tackling this should be the metric of success for privacy law is a question that has been in general loudly ignored.

This brings us to data governance (Viljoen, 2021). Data governance law — defined by Viljoen as "the legal regime that governs how data about people is collected, processed, and used"— offers an exciting path for overcoming much of the criticism toward data protection by exploring collective self-determination. If responding to the tyranny of the minority might be over-indexing for privacy law, it would be precisely under the remit of data governance's aim "to account for population-level interests in the digital economy" (Viljoen, 2021, p. 653). It should be noted, however, that proponents of data governance have not addressed those pre-digital instances of obtaining population information from a limited number of members. 218 ↑

Now, the approach of data governance can productively offer avenues for collective self-determination in situations where the affected collective can be discerned easily and with regards to a correspondingly limited set of data practices (e.g. Salomé Viljoen's Waterorg, a hypothetical water management authority for a drought-afflicted region tracking water consumption data "to ensure water will be distributed fairly and responsibly as it becomes scarcer" (Viljoen, 2021, p. 635)). We can see how some data processing that could potentially be impractical under current privacy law might be beneficially adopted with an institutional arrangement that allows for collective self-determination. ↓ 219

Such unleashing shows data governance in tension with privacy lawand as its new and improved replacement. Even if we ignore that, however, the project of data governance could render irrelevant privacy law as characterized by the pragmatic approach. If privacy is to be valued only instrumentally (Richards, 2022, p. 68) and measured by the impacts it has for a particular social practice (Solove, 2002, p. 1144), then data governance and privacy law share the same success criteria: which data processing (or abstention from processing) produces the best societal outcome. This suggests a competition between two regulatory frameworks — one which privacy law is likely to lose. It could hardly expect to have a better answer to that question about societal outcomes than one backed by the democratic imprimatur of the self-government claimed by data governance. Data governance would then make privacy law redundant and antiquated, no more than a cumbersome compliance exercise.

There are likely to be serious challenges to data governance in practice, particularly when the affected population cannot plausibly be thought to deliberate about its own interests, because individuals don't see themselves as members of a community— suppose, for instance, that we are talking about the class of people with type A blood. This is not so much an objection to the data governance approach itself as perhaps a limitation to it.

[6] *See* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.510(b) (2016).

A more serious problem with data governance presents itself if proponents assume that this approach would replace all privacy considerations. Even when the affected population is clearly defined and can deliberate as a community, privacy interests might be dramatically different across various groups. It might be the case, for instance, that a proposed smart-city data processing would implicate practices of a religion professed by a minority of the population.

This shows that data governance and privacy law not only complement each other, as Lisa Austin notes,[7] but also that the latter might *restrict* the options available for collective self-government sought by the former. This should not be surprising if we think about democratic data governance just as we do about government generally, where constitutional rights impose boundaries to what even democratically elected officials can require.

An objection to the example above might suggest that what is at stake is a different right, namely religious freedom, so that, in cases where only the right to privacy is implicated, data governance schemes would control. This need not be so, nor would questions only be raised with regard to specific social groups.

Covid-19 contact-tracing apps are a good illustration. Even though the importance of contact-tracing was established and a decentralized approach was developed that minimized data processing, the European Data Protection Board (EDPB) still advised that such apps should be voluntary, "a choice that should be made by individuals as a token of collective responsibility", emphasizing the importance of "individual trust" (Jelinek, 2020). While there might be disagreement about whether this conception of the right to privacy is compelling, this shows that there is still much theoretical work to be done.

219 ↑
↓ 220

IV. CONCLUSION

We might say an ambitious and encompassing legislation which has ceded with theoretical vexations vastly expanded the preserves of privacy law, but has been lacking in addressing a number of concerns regarding data processing. The perhaps natural culmination of the pragmatic turn and the privacy disconnect is a turn away from privacy and toward fresh thinking on data governance. That is the crossroads the right to privacy is at: at the same time its reach and significance arguably have attained unprecedented levels, it seems to be in the brink of being left behind like an old toy which has outlived its owner's infancy.

[7] "Privacy remains of vital importance." Austin (2022, p. 305)

REFERENCES

Austin, L. (2022). From privacy to social legibility. *Surveillance & Soc'y*, *20*(3), 302–305. https://doi.org/10.24908/ss.v20i3.15762

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: frameworks for engagement* (pp. 44–75). Cambridge Univ. Press. https://doi.org/10.1017/cbo9781107590205.004

Benn, S. I. (1984). *Privacy, freedom, and respect for persons* (1st ed., pp. 223–244). Cambridge. https://doi.org/10.1017/cbo9780511625138.009

Bennett, C. J. (1992). *Regulating privacy*. Cornell Univ. Press.

Bieker, F. (2022). *The right to data protection: individual and structural dimensions of data protection in EU law* (34). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-503-4

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: an answer to dean Prosser. *N.Y. U. L. Rev.*, *39*(6), 962–1007.

Board, E. D. P. (2020, May). *Guidelines 05/2020 on consent under regulation 2016/679*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Calo, R. (2011). The boundaries of privacy harm. *Ind. L.J.*, *86*(3), 1131–1162.

Chander, A., Kaminski, M. E., & McGeveran, W. (2021). Catalyzing privacy law. *Minn. L. Rev.*, *105*(4), 1733–1802.

Citron, D. K. (2022). *The fight for privacy: protecting dignity, identity, and love in the digital age*. W. W. Norton.

Conger, K., & Chen, B. X. (2022). Apple's privacy changes could cost Meta big time. *N.Y. Times*, 1. https://www.nytimes.com/2022/02/03/technology/apple-privacy-changes-meta.html

Flaherty, D. H. (1991). On the utility of constitutional rights to privacy and data protection. *Case W. L. Rev.*, *41*(3), 831–855.

Gavison, R. (1984). *Privacy and the limits of law* (F. D. Schoeman, Ed.; pp. 346–402). Cambridge. https://doi.org/10.1017/cbo9780511625138.017

Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Comput. L. & Sec. Rev.*, *29*(5), 522–530. https://doi.org/10.1016/j.clsr.2013.07.005

Gutwirth, S., & Hert, P. D. (2006). Privacy, data protection and law enforcement: opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61–104). Intersentia.

Hadjimatheou, K. (2017). Surveillance technologies, wrongful criminalisation, and the presumption of innocence. *Phil. & Tech.*, *30*(1), 39–54. https://doi.org/10.1007/s13347-016-0218-2

Hartzog, W. (2021). What is privacy? That's the wrong question. *U. Chi. L. Rev.*, *88*(1), 1677–1688.

Hoboken, J. van. (2019). The privacy disconnect. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms* (pp. 255–284). The MIT Press.

Jelinek, A. (2020, April). *Ref: OUT2020-0028*. https://edpb.europa.eu/sites/default/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *Int'l Data Priv. L.*, *3*(4), 222–228. https://doi.org/10.1093/idpl/ipt017

Kollnig, K., Shuba, A., Kleek, M. V., Binns, R., & Shadbolt, N. (2022). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. *2022 ACM Conf. On Fairness, Accountability, & Transparency*, 508–520. https://doi.org/10.1145/3531146.3533116

Koops, B.-J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *U. Pa. J. Int'l L.*, *38*(2), 483–575.

Marmor, A. (2015). What is the right to privacy? *Phil. & Pub. Affairs*.
Pałka, P. (2020). Data management law for the 2020s: the lost origins and the new needs. *Buff. L. Rev.*, *68*(2), 559–640.
Party, A. 29. D. P. W. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
Prosser, W. L. (1960). Privacy. *Calif. L. Rev.*, *48*(3), 383–423.
Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *L., Innovation & Tech.*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176
Rachels, J. (1975). Why privacy is important. *Phil. & Pub. Affairs*, *4*(4), 323–333.
Regan, P. M. (1995). *Legislating privacy*. Univ. of N.C. Press.
Reiman, J. H. (1976). Privacy, intimacy, and personhood. *Phil. & Pub. Affairs*, *6*(1), 26–44.
Richards, N. M. (2006). The information privacy law project. *Geo. L.J.*, *94*(4), 1087–1140.
Richards, N. M. (2022). *Why privacy matters*. Oxford Univ. Press.
Richards, N. M., & Hartzog, W. (2017). Privacy's trust gap: a review. *Yale L.J.*, *126*, 1180–1224.
Richards, N. M., & Solove, D. J. (2007). Privacy's other path: recovering the law of confidentiality. *Geo. L.J.*, *96*(1), 123–182.
Richards, N., & Hartzog, W. (2019). The pathologies of digital consent. *Wash. U. L. Rev.*, *96*(6), 1461–1503.
Richardson, M. (2017). *The right to privacy: origins and influence of a nineteenth-century idea*. Cambridge Univ. Press. https://doi.org/10.1017/9781108303972
Roessler, B. (2005). *The value of privacy* (R. D. V. Glasgow, Tran.). Polity.
Roessler, B. (2017). Privacy. *Proc. Aristotelian Soc'y*, *117*(2), 187–206. https://doi.org/10.1093/arisoc/aox008
Scanlon, T. (1975). Thomson on privacy. *Phil. & Pub. Affairs*, *4*(4), 315–322.
Schoeman, F. D. (Ed.). (1984a). *Philosophical dimensions of privacy: an anthology*. Cambridge.
Schoeman, F. D. (1984b). Privacy: philosophical dimensions. *Am. Phil. Q.*, *21*(3), 199–213. https://doi.org/10.5406/illinois/9780252036347.003.0011
Schwartz, P. M., & Peifer, K.-N. (2010). Prosser's "Privacy" and the German right of personality: are four privacy torts better than one unitary concept? *Calif. L. Rev.*, *98*(6), 1925–1987. https://doi.org/10.2307/25799959
Solove, D. J. (2002). Conceptualizing privacy. *Calif. L. Rev.*, *90*, 1087–1155.
Solove, D. J. (2006). A taxonomy of privacy. *U. Pa. L. Rev.*, *154*(3), 477–564.
Solove, D. J. (2008). *Understanding privacy*. Harvard Univ. Press.
Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harv. L. Rev.*, *126*, 1880–1903.
Solow-Niederman, A. (2022). Information privacy and the inference economy. *Nw. U. L. Rev.*, *117*(2). https://doi.org/10.2139/ssrn.3921003
Thomson, J. J. (1975). The right to privacy. *Phil. & Pub. Affairs*, *4*(4), 295–314.
Tugendhat, M. (2017). *Liberty intact: human rights in English law*. Oxford Univ. Press.
Viljoen, S. (2021). A relational theory of data governance. *Yale L.J.*, *131*(2), 573–654.
Waldman, A. E. (2018). *Privacy as trust*. Cambridge Univ. Press. https://doi.org/10.1017/9781316888667
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harv. L. Rev.*, *4*(5), 193–220. https://doi.org/10.2307/1321160
Whitman, J. Q. (2004). The two Western cultures of privacy: dignity versus liberty. *Yale L.J.*, *113*(6), 1151–1221. https://doi.org/10.2307/4135723