Privacy as Antipower: In Pursuit of Non-Domination

*Bryce Clayton Newell**

Privacy and domination have something of a difficult history. On one hand, on some accounts, privacy can act as a shield against domination and arbitrary interference by others, including the state, in individual lives.[1] On the other hand, privacy can also be seen to promote domination in some contexts by shielding more private forms of discrimination and abuse from public scrutiny.[2] Indeed, a feminist critique of privacy emphasizing 'problems of domination' would suggest 'that a life of liberty properly includes both privacy and freedom from privacy'.[3] To some extent, the conflict between these arguments may be seen as a function of differing perspectives, life experiences, or political philosophies,[4] but they may also be a consequence of the fact that defining privacy adequately, especially across disciplines and contexts, has proven to be such a difficult task.[5] Likewise, the overlap between privacy (as a concept and as a legal right) and data protection rights is not perfect, as each encompasses important elements that extend beyond the other. In the end, I propose that privacy, properly conceptualised, can indeed function as 'a particularly useful instrumental means of supporting the goal of maintaining individual liberty from (…) domination'[6] while also accounting for the potentially discriminatory and subjugating effects targeted by feminist concerns. Specifically, I argue that privacy is valuable, at least in large part, because it is instrumental to achieving liberty (defined as the absence of the possibility of domination).[7] That is, privacy effectuates freedom in a variety of contexts, and it does so by resisting domination.

The rule of law serves to protect individuals against 'excessive and arbitrary domination'.[8] As Roberts has noted, 'there are various conceptions of domination, [although] at the root of each is the idea that we suffer some diminution in our freedom where

* Bryce Clayton Newell, JD, PhD, Assistant Professor in the School of Information Science at the University of Kentucky. His research focuses on the intersections between law, technology, surveillance, and society. For correspondence: <brycenewell@uky.edu>.

1 See, eg, Andrew Roberts, 'A republican account of the value of privacy' (2015) 14(3) European Journal of Political Theory 320-44; Bryce Clayton Newell, *Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy* (Unpublished doctoral thesis, University of Washington 2015).

2 See Judith Wagner DeCew, 'The Feminist Critique of Privacy: Past Arguments and New Social Understandings' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 88–9; Anita L Allen, *Unpopular Privacy: What must we hide?* (Oxford University Press 2011) 11; Catharine MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) 191.

3 Allen (n 2).

4 Andrew Roberts, 'Privacy and Political Theory' (Melbourne Legal Studies Research Paper No 690, 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2476761> accessed 19 February 2018.

5 See, eg, Bert-Jaap Koops et al, 'A Typology of Privacy' (2017) 38(2) University of Pennsylvania Journal of International Law 483-575, 491.

6 Newell (n 1) 27.

7 For an elaboration of this argument, see Newell (n 1).

8 Paul de Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power' in Erik Claes, Antony Duff, and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 61–104, 65.

others have unconstrained power to interfere in our decision-making'.[9] In this foreword, I focus specifically on a theory of domination proposed by Philip Pettit, but there are a number of other plausible theories that could be harnessed for similar purposes.

As conceptualised by Pettit, domination occurs when an agent has the actual capacity to exert 'a certain power over the other: in particular the power to interfere in the affairs of the other and to inflict a certain damage'.[10] More recently, Pettit offered the following formulation: 'Someone, A, will be dominated in a certain choice by another agent or agency, B, to the extent that B has a power of interfering in the choice that is not itself controlled by A'.[11] Importantly, this republican conception of liberty is not concerned directly with *acts* of subjugation, but rather the power relationships that make acts of subjugation possible. As stated quite clearly by Ivison, 'the bare potential for interference threatens my liberty, not only the likelihood or probability of its exercise'.[12] On this account, domination is present when an agent has the actual capacity to interfere, arbitrarily and with impunity, with choices the dominated agent otherwise has the capacity to make. This characterisation of domination would encompass both forms of intrusive state surveillance into private affairs as well as the private relationships between domestic partners. We should work to reduce domination, in all its forms, and equalise power in each of these circumstances. The point here is that we should organise social, organisational, and political relations so as to maximise what Pettit calls 'antipower'—that is, 'what comes into being as the power of some over others—the power of some over others in the sense associated with domination—is actively reduced and eliminated', [13] granting the individual the power to essentially 'command noninterference'.[14] Thompson, though offering a critique of Pettit's view, argues similarly that, rather than just focusing on eliminating domination from others, we should address the very 'architecture [and] arrangement of social institutions (…) ensuring that society is arranged in such a way as to orient social power not only negatively, but positively as well'.[15]

Privacy, a 'core value that limits the forces of oppression'[16] is an important element in the pursuit of non-domination. As explained clearly by Roberts,

> the value of privacy for republicans lies in its capacity to shield individuals from the threat of domination. A consequence of loss of one's privacy is that others may acquire dominating power – the capacity to interfere in one's decisions on an arbitrary basis.[17]

---

9 Andrew Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications' (2015) 78(3) Modern Law Review 522–548, 544.

10 Philip Pettit, 'Antipower' (1996) 106(3) Ethics 576–604, 578.

11 Phillip Pettit, *On the People's Terms: A Republican Theory and Model of Democracy* (Cambridge University Press 2012) 50.

12 Duncan Ivison, 'Republican Human Rights?' (2010) 9(1) European Journal of Political Theory 31–47, 34–5.

13 Pettit (n 6) 588; Newell (n 1) 26.

14 Pettit (n 6) 589; Newell (n 1) 26.

15 Michael J Thompson, 'Reconstructing republican freedom : A critique of the neo-republican concept of freedom as non-domination'(2013) 39(3) Philosophy and Social Criticism 277–98, 278.

16 Adam D Moore, 'Privacy, Speech, and the Law' (2013) 22(1) Journal of Information Ethics 21–43.

17 Roberts (n 1) 321.

This conception of privacy is consistent with the claims that privacy is 'a core human value necessary for human well-being or flourishing'.[18] Combining these two conceptualisations of the value of privacy, we can see that privacy is 'directly connected to human flourishing precisely because it reduces domination and increases antipower'.[19] This dual focus on promoting human flourishing and reducing domination find support in privacy theories that would decrease unwanted visibility—whether conceptualised as the desire for separation from others,[20] obscurity,[21] semantic discontinuity,[22] or the mosaic theory.[23]

Information facilitates the acquisition of power and makes some forms of domination possible.[24] Information privacy, as an 'overlay' that derives its substance from a variety of underlying types of privacy,[25] resists domination because it restricts the flow of information and therefore limits the ability of others to acquire the capacity to interfere. Concerns about surveillance, the collection of (personal) information, and power manifest as elements of a broader politics of information, described as 'the manipulation of information access for political gain'[26] and as 'the use of information and information processing as a decisive tool of power-making'.[27] It is not at all coincidental that surveillance, defined by David Lyon as the 'focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction'[28] is strikingly similar to this concept of information politics. Likewise, *vision* (as a manifestation of surveillance) has been described by Brighenti as 'a sense of power,' while 'visibility is precisely the complex field where the visible and the articulable coexist'.[29] Indeed, it is clear that visibility has clear connections to exposure, recognition, subjectification, and objectification.[30] As stated convincingly by Julie Cohen, 'freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship' and 'privacy… is an indispensable structural feature of liberal democratic political systems'.[31] That is, robust and thoughtful priva-

18 Adam D Moore, *Privacy Rights: Moral and Legal Foundations* (Pennsylvania State University Press 2010) 143.

19 Newell (n Error: Reference source not found) 31 ['Roberts also recognizes (…) that there is no reason to think that republicans would reject the claim that it is part of human nature to seek a degree of separation from others in some circumstances, and that such separation is essential to human flourishing', citing Roberts (n Error: Reference source not found), 328 (internal quotations omitted)].

20 See, eg, Moore, 'Privacy, Speech, and the Law' (n 6); Alan F Westin, *Privacy and Freedom* (Atheneum 1967).

21 See, eg, Woodrow Hartzog and Evan Selinger, 'Surveillance as Loss of Obscurity' (2015) 72 Washington & Lee Law Review 1343–87; Woodrow Hartzog and Frederic Stutzman, 'Obscurity by Design' (2013) 88 Washington Law Review 385–418; Woodrow Hartzog and Frederic Stutzman, 'The Case for Online Obscurity' (2013) 101(1) California Law Review 1–49; De Hert and Gutwirth (n 8) 67.

22 Julie E Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904–1933; Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012).

23 See, eg, Christopher Slobogin, 'Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory' (2012) 8 Duke Journal of Constitutional Law & Public Policy 1–37.

24 See Bryce Clayton Newell, 'Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control' (2014) 31 Government Information Quarterly 421–431, 422.

25 See Koops et al (n 4) 566.

26 Paul T Jaeger, 'Information policy, information access, and democratic participation: The national and international implications of the Bush administration's information policies' (2007) 24 Government Information Quarterly 840–859, 851.

27 Manuel Castells, *Communication Power* (Oxford University Press 2009) 197.

28 David Lyon, *Surveillance studies: An overview* (Polity Press 2007) 14.

29 Andrea Brighenti, 'Visibility: A category for the social sciences' (2007) 55(3) Current Sociology 323–42, 328-9.

30 ibid 329.

31 Cohen, 'What Privacy Is For' (n 22) 1905; see also Roberts (n 1).

cy rights can serve as a bulwark against subjugation and domination by the state as well as by private actors.

However, current privacy and data protection rights are not always adequate. The limited and sectoral protections for privacy rights in the United States, for example, are evidence that much work needs to be done. It is within this context that legal concepts like the mosaic theory—or that the sum of aggregated pieces of information about a person, in terms of privacy intrusion, is more than merely the sum of its parts—have been introduced within the Fourth Amendment (search and seizure) context in the United States. Likewise, arguments for encoding 'obscurity'[32] into law and the design of technological artifacts are increasingly relevant to promoting privacy as a mechanism of antipower. Similarly, when Cohen describes her concept of 'semantic discontinuity', referring to 'gaps and inconsistencies within systems of meaning, and to a resulting interstitial complexity that leaves room for the play of everyday practice'[33] she is arguing that we should encode 'gaps in enforcement and in systems of surveillance and control'.[34] As 'the opposite of seamlessness,' semantic discontinuity refers to 'discontinuity in forms of social and technical power'[35]—in practical terms, 'gaps and imperfections in systems of control and surveillance'.[36] The function of what De Hert and Gutwirth refer to as 'opacity tools', which serve to 'shield individuals against state interference' has also been likened to that of the 'first generation of human rights'.[37]

To some, these recommendations might seem extreme, unnecessary, or impossible. However, practical, successful, real-life examples do exist. Harnessing privacy rights as a tool in the fight to limit domination is possible. As a case in point, Roberts argues convincingly that the European Court of Justice's decision in the *Digital Rights Ireland* case,[38] invalidating data retention obligations promulgated by Member State governments under the authority of the European Data Retention Directive,[39] is an instance where a law that 'confer[red] dominating power' was deemed to violate human rights-based interests in personal privacy.[40] Similarly, privacy-related decisions by the European Court of Human Rights, such as the *Von Hannover v Germany* case,[41] in which the Court held that the right to private life under Article 8 of the European Convention on Human Rights extended to private activities (even when they occur in public spaces

32 See references at (n 19).

33 Cohen, *Configuring the Networked Self* (n 2) 224.

34 Jack M Balkin, 'Room for Maneuver: Julie Cohen's Theory of Freedom in the Information State' (2012) 6(1) Jerusalem Review of Legal Studies 79–95, 81.

35 Cohen, *Configuring the Networked Self* (n 2) 224.

36 Michael Rich, 'Limits on the Perfect Preventative State' (2014) 46 Connecticut Law Review 883–935, 928.

37 De Hert and Gutwirth (n 8) 67.

38 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communication* [2014] ECLI:EU:C:2014:238.

39 Council Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54.

40 Roberts (n 9).

41 *Von Hannover v Germany* App nos 40660/08 and 60641/08 (ECtHR, 2004).

and even for otherwise public figures), enable the sort of boundary management and obscurity functions called for above.

Indeed,

> modern surveillance capabilities, including increasingly sophisticated forms of *vision*, the aggregation of personal information across time and disparate systems (…) and the permanence of digital memory, all point to a need to rethink how we structure privacy rights, from both a moral and legal perspective.[42]

This is true across a wide variety of contexts, from criminal investigations to the steady increase in cases of digital/online extortion, interfamilial (spousal/partner) surveillance, and so-called revenge or nonconsensual pornography. Across these contexts, and beyond, privacy has the 'capacity to shield individuals from the threat of domination'[43]—both within the public and private spheres of life. We, as scholars, lawyers, legislators, and policy-makers, ought to work to ensure this capacity is realized.

42 Newell (n 1) 160.

43 Roberts (n 1) 321.