Law and Philosophy
https://doi.org/10.1007/s10982-024-09500-9

LISA M. AUSTIN

DIGITAL POWER AND *LAW'S RULE*

(Accepted 16 March 2024)

ABSTRACT. In *Law's Rule*, Gerald Postema provides a robust theoretical framework of the rule of law that technology scholars can use to analyze power in the digital world. He articulates how the rule of law can be concerned with private power, and not just public power. His emphasis on the ethos of fidelity allows us to see how the rule of law of law may be degraded in the digital era through the erosion of the informal institutions and practices needed to sustain the rule of law. In addition to outlining these contributions, this paper argues that Postema's account of digital power needs to focus more on digital power structures rather than digital power wielding, that digital power structures erode many informal constraints on power, and that addressing sociotechnical systems might require rethinking law's distinctive instrumentalities in order to embrace the use of digital technologies to increase transparency and compliance.

I. INTRODUCTION

Analyzing how power is constructed, distributed, legitimized, and constrained in the digital world is an increasing focus of the broadly interdisciplinary scholarship examining contemporary data practices and digital technologies.[1] In this comment I hope to persuade such scholars to engage with Gerald Postema's analysis of power and the rule of law in *Law's Rule*. In addition to providing a powerful account of the rule of law, Postema applies his framework to pressing contemporary challenges including the challenge of digital power, the prospect of AI replacing law, and the issue of digital power's global

[1] See, for e.g., Julie Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford and New York: Oxford University Press, 2019); Shoshana Zubboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: Public Affairs, 2019); Seth Lazar, ''Power and AI: Nature and Justification'', in Justin Bullock and Johannes Himmelreich (eds.), The Oxford Handbook of AI Governance (Oxford and New York: Oxford University Press); M Micheli et al., ''Emerging Models of Data Governance in the Age of Datafication'', Big Data & Society 7(2) (2020), https://doi.org/10.1177/2053951720948087.

Published online: 14 June 2024

reach. Two aspects of his account are particularly helpful in relation to these debates. The first is his account of power and its ability to address the problem of *private* power. The second is his account of the relationship between the rule of law and 'fidelity', or the ethos of the political community and the ways in which this can be eroded through the practices of digital power. Both his account of power and his account of fidelity provide technology scholars with a rich theoretical framework with which to analyze, and ground, many different types of legal interventions in the digital world.

In addition to outlining these contributions, I also point to a number of areas where *Law's Rule* falls short in addressing digital power. None of my criticisms undermine Postema's overall account, and defence, of the rule of law. Instead, I use Postema's framework to point to areas where the analysis offered does not go far enough.

I push on three aspects of Postema's account of digital power. The first is on his emphasis on power-wielders, or *agents* who dominate, rather than the power structures that place agents in the position to dominate. The second to some extent follows from the first. Because of Postema's emphasis on digital power wielding, he does not pay enough attention to the way in which digital power structures contribute to the erosion of many of our informal constraints on power. The third addresses his critique of the use of AI in law. Although I agree with much of what he says about *replacing* our traditional legal toolkit with AI, he does not address the important question of whether we can adopt some of the tools of digital technology in aid of rule of law values. These three areas where Postema's account is underdeveloped leaves us with a diminished sense of law's potential responses to digital power. I offer suggestions as to how we might develop a more robust account and what kinds of responses such an account would call for.

II. POSTEMA'S ACCOUNT OF THE RULE OF LAW AND THE CHALLENGE OF DIGITAL POWER

Postema offers a rich account, and defence, of the rule of law. He argues that, historically, its animating values have been the constitution and constraint of power.[2] For him, the rule of law offers protection and recourse from arbitrary power through the means of

[2] Law's Rule at p. 3.

law and its distinct toolkit, a toolkit heavily informed by the nature of law as a deliberative practice. In this section I will outline some of the key features of his account and indicate how they help him provide a number of important insights in relation to digital power.

A. Private Power

The emphasis in rule of law scholarship is on the ways in which the rule of law might constitute and constrain *public* power, such as state action, and provides fewer resources with which to think about private power. This leaves many scholars concerned with private power to make arguments to the effect that, in some circumstances, private power is analogous to public power.[3]

One of the reasons for the lack of attention to private power lies with how the problem of arbitrary power is framed. For example, for Raz the rule of law is concerned with the arbitrary exercise of power through the instrumentality of the law.[4] The rule of law is a concern once the state decides to use the law as an instrument but does not assist us when power is exercised in other ways and cannot help us understand when and whether the state should use law, rather than other means, to achieve its ends. In contrast, Postema offers us an account where the rule of law is concerned with constraining the arbitrary exercise of power no matter how that power is exercised. He roots its value in an ideal of association he calls 'membership'.[5] This provides a basis for arguing that the arbitrary exercise of private power raises rule-of-law concerns and that these concerns can justify legal interventions. These interventions can take the form of legal constraints on power or they can take the form of law's role in constituting and legitimizing power.[6]

Postema argues that power has two aspects: capacity and position.[7] The first refers to the ability to get someone to do something they might not otherwise do. The latter does not involve getting

[3] There is a growing literature on platform governance that takes this approach to the analysis of platform power. See, for example, Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech", Harvard Law Review 131(6) (2018): pp. 1598–1670.

[4] Joseph Raz, "The Rule of Law and Its Virtue", The Law Quarterly Review 93 (1977): pp. 195–211.

[5] But see also Jeremy Waldron, "The Concept and the Rule of Law", Georgia Law Review 43(1) (2008): pp. 1–61; Robin L. West, Re-Imagining Justice: Progressive Interpretations of Formal Equality, Rights, and the Rule of Law (Ashgate, Aldershot, 2003).

[6] Law's Rule at p. 11.

[7] *Ibid*. at pp. 23–24.

others to do things but refers to legally or socially created privileges such as the power of an owner to sell their home.[8] In general, the rule of law is concerned with power as *capacity* and, in particular, the 'the socially embedded capacity of one agent to influence another in circumstances of marked dependency'.[9] Importantly, power need not be exercised in order for the rule of law to be concerned with it, it need only exist[10], as the existence of power can itself influence others. The rule of law is also concerned with power as position. For example, Postema argues that a president would abuse his power as president by pardoning friends and relatives. In this latter case, the problem is not influencing others but treating 'the law with contempt'.[11] However, Postema pays much less attention to this, and the book centers its analysis on power as capacity and power-wielders as those who exercise this capacity.

The rule of law can also be concerned with structures of power. However, Postema cautions that it is misleading to view such structures 'as analogues of agents who exercise power', for it is agents who dominate others and structures put those agents in positions to dominate.[12] Consider Postema's example of the power of banks, taken from Steinbeck's novel *The Grapes of Wrath*. Agents of the bank seek to disclaim responsibility for delivering eviction notices to the farmers by arguing that it is the bank, not them, that is responsible. Postema argues:

> The bank's institutional frame makes possible the exercise of power, but agents, employees, directors, and officers exercise the power. As responsible agents, they are – or should be – held accountable for their actions. If they are not held accountable, because a corporate veil is thrown over their activities, then their exercise of power is recognizably arbitrary, worthy of condemnation, and worthy of the concern of the rule of law. Moreover, the rule of law is equally concerned with the structures that constitute and sustain that power.[13]

Structures do not wield power, agents do. However, structures create the conditions for that wielding of power and therefore may also be condemned from the point of view of the rule of law. Although Postema does not directly discuss this, we could also argue that structures that involve legally created positions and privileges that do not have sufficiently robust protections against their abuse

[8] *Ibid*. at p. 24

[9] *Ibid*. at p. 25 (he also discusses power as position, but this is less relevant to data power).

[10] *Ibid*. at p. 26.

[11] *Ibid*. at p. 28.

[12] *Ibid*. at p. 28.

[13] *Ibid*. at p. 31.

thereby also create the conditions for the wielding of power.

Digital power fits within Postema's understanding of power as capacity, as data and the digital technologies that allow its collection and analysis influence others. Indeed, digital power is 'immaterial, ephemeral, yet its ability to penetrate our lives and manipulate our behavior dwarfs that of more familiar forms of power'.[14] Its concentration in the hands of a small number of data giants, largely without accountability, creates the circumstances of 'marked dependency' that raise rule-of-law concerns.[15] Postema also argues that digital power represents something new in how it is wielded. Traditionally, we model power through a direct relationship between a power wielder and the person subject to this power. Postema calls this the one-to-one model of power. However, digital power cannot be modeled in this way. Through surveillance and manipulation, digital power wielders 'influence the architecture of deliberation and choice' of those who are subject to this power but they do so through the aggregation of data and the application of AI technologies to this aggregated data.[16] To come to grips with this, he argues that we need an 'aggregation model' that can understand the layers of technical and economic intermediation involved.[17] While this is a key insight, I argue below that it also sets the stage for a key tension in Postema, which is the tension between agents and structures.

Power becomes a concern for the rule of law when it is arbitrary. Postema argues that power can be exercised in an arbitrary manner *even if* it is exercised according to reason and is entirely predictable. For him, arbitrary power means power that is unilaterally exercised, where only the perspective of the power wielder matters.[18] Arbitrary power is also unaccountable because such power wielders are not answerable to anyone for how they exercise their power.

By providing a broad theory of arbitrary power and its relationship to the rule of law, Postema offers theorists of digital power some important and fundamental tools. For example, example, a rule-of-law perspective offers an easy critique of internal governance

[14] *Ibid.* at p. 263.
[15] *Ibid.* at pp. 263–264.
[16] *Ibid.* at p. 271.
[17] *Ibid.* at p. 267.
[18] *Ibid.* at p. 29.

regimes as being unaccountable in the relevant way. Whether it is internal ethics committees or other modes of self-regulation, they fail in being accountable to the relevant public.[19] Because Postema has a broad conception of digital power, he criticizes solutions such as user-focused governance, antitrust law and the GDPR as being too limited.[20] As the next section outlines, Postema's analysis of the core principles of the rule of law – and in particular 'fidelity' – provide the basis for more detailed proposals.

B. Fidelity and the Core Principles

If the area of concern for the rule of law is the arbitrary exercise of power, then what does the rule of law require as a response? Postema argues that there are three principles that form the core of the rule of law: sovereignty, equality, and fidelity. He describes these principles as follows

> Sovereignty demands that those who exercise ruling power *govern with* law (legality), and that law *governs them* (reflexivity), and only acts that are ordained by law are legitimate (exclusivity). Equality requires that law's protection and recourse be made available on an equal basis for all who are also bound by it. Fidelity requires that all of the members of the political community, and not merely the legal or ruling elite, take responsibility for holding each other, and especially law's officials, accountable under law.[21]

Postema draws upon these principles to argue that law's distinctive instrumentalities can constrain digital power. These instrumentalities include:

> setting public standards for the exercise of digital power, devising institutional mechanisms and procedures for public assessment of it, and enabling and mobilizing informal public participation in this accountability-holding.[22]

Some options that he endorses include algorithmic accountability – including transparency, explainability, justification, certification of accuracy and compliance with normative standards, and mechanisms for mitigating errors and harms – as well as the establishment of new types of special agencies that can set standards for data practices.[23] Many of these specific proposals exist in the law and technology literature but Postema offers an important rule-of-law grounding for them.

[19] *Ibid.* at p. 280.

[20] Ibid. at Chapter 13.

[21] *Ibid.* at p. 334.

[22] *Ibid.* at p. 277.

[23] *Ibid.* at p. 286.

Postema also makes a number of more novel contributions arising from his analysis of fidelity. Postema argues that the 'most fundamental thesis' of his book is that we need to look beyond the formalities of law (its rule, procedures, and institutions) and see the rule of law's 'animating spirit', which he describes as

> the ethos of the people who seek the rule of law for their community. Law rules in a political community only when there is in that community a deeply rooted ethos of fidelity. Fidelity is practiced when all members of the community, official and nonofficial alike, take responsibility for holding each other to account under the law.[24]

This horizontal accountability must be supported through civil society institutions. He singles out two types of critical resources. The first is public spaces where individuals can learn to trust in others and in the possibilities of collective action. The second is the 'networks of associations, organizations, and institutions that transform individual energy into disciplined and effective collective effort over time'.[25]

Postema points out that some of this informal infrastructure is in peril in the digital age in a number of ways. He argues that an ethos of fidelity can be eroded through external forces such as 'the corrosive effects of digital technology'.[26] This includes the degradation of public discourse through misinformation and also includes 'the shrinkage of public space, of public *place* and public *practice*'.[27] Interactions in public spaces are important for the development of generalized trust, without which fidelity is very difficult.[28] Digital platforms undermine public deliberative space through their control of content (including misinformation) and through the effect of our social life migrating to digital platforms instead of physical public spaces.[29]

In these ways, Postema's analysis of the core principles of the rule of law provides theorists with an important set of tools for both analyzing the effects of digital technology and for justifying regulatory interventions. While Postema acknowledges that the rule of law is related to a broader set of values such as democracy and human

[24] *Ibid.* at p. 334.
[25] *Ibid.* at p. 336.
[26] *Ibid.* at p. 161.
[27] *Ibid.* at p. 164, italics in original.
[28] *Ibid.* at p. 164.
[29] *Ibid.* at pp. 275–276.

rights[30], the rule of law is a kind of ground norm. Despite disagreement about specific norms within a state, and between states, there can be a consensus that the digital realm should be one that is subject to the rule of law.

III. CRITICALLY ASSESSING POSTEMA'S ACCOUNT OF DIGITAL POWER

A. Power Wielding and Power Structures

Postema's insight that the digital realm requires a model of aggregate power, rather than a one-to-one model, is very important. As he argues, '[a]ny model that represents the basic normative relationship in digital space exclusively as one between discrete individuals and a digital company … fails to account for the full range of activities and relationships operating in the digital world'.[31] The main insight he develops regarding aggregation is that the aggregation of data is what affects individuals, even though that data is often about other people and not necessarily identifiable. Postema also recognizes that an individual might be subject to 'a decentralized aggregate of potential wielders'[32] and that the harms involved in digital power-wielding might be public harms[33] rather than individual ones.

However, what this does not adequately account for is the fact that data and data aggregation depend upon complex socio-technical systems embedded within larger legal, economic, and political structures.[34] The role of structures and systems in a model of aggregate power remains unclear. I want to return to Postema's explicit comments about structural power and raise some questions about how this maps onto the digital sphere, for I think that it keeps us from fully appreciating the potential role of law in reigning in digital power.

Recall that for Postema, it is *agents* who dominate – structures place agents in the position to dominate. This is important, for it is agents whom we call to account. On Postema's example of the bank, it is the bank employees who exercise agency and are therefore accountable and should not be permitted to evade this accountability

[30] See Chapter 5.
[31] *Ibid.* at p. 288.
[32] *Ibid.* at p. 27.
[33] *Ibid.* at p. 272.
[34] See Cohen and Zuboff, *supra* note 1.

by pointing to the impersonal structure of the bank. It is ridiculous, he argues, for the bank employees to claim that 'The Bank' was throwing the farmers off the land and not any person. Similarly, he argues that it would be ridiculous in the digital age to make analogous claims about digital power wielders. Postema points out that there are many different persons who wield digital power and can be held responsible:

> Actors at various levels – coders, engineers, computer scientists, data controllers and processors, data brokers and marketers, and ultimately corporation leaders – are all agents capable of bearing moral and legal responsibility.[35]

This is not to say that the rule of law is unconcerned with systems and structures. Even in his early discussion of the bank example, Postema writes that 'the rule of law is equally concerned with the structures that constitute and sustain that power'.[36] This is reiterated at other points in the book but is not really developed.[37] And the bank example suggests that what we should primarily do when faced with a claim about the power relations embedded within an impersonal institutional framework is to look beyond this structure to the people who exercise agency within it.

The problem with the underdevelopment of what it might mean for the rule of law to concern itself with structure is that Postema places his focus on digital giants. In his analysis of digital power, he argues that the rule of law is particularly concerned when data power is concentrated in the hands of a few power wielders.[38] Moreover, when addressing how the law might respond and constrain the power of the new digital giants, he focuses on a fairly traditional view of 'law's distinctive instrumentalities'. The emphasis is therefore on the (human) agents and the exercise of wielding digital power; the response demanded is that we create public standards for the exercise of this power and public processes of accountability-holding.

What might an alternative rule-of-law agenda look like in relation to digital power structures? Let me return to Postema's bank example and outline why Postema is partially wrong in his discussion of agency and the bank, and how understanding this can point us in a

[35] Law's Rule at p. 270.
[36] *Ibid.* at p. 31.
[37] *Ibid.* at p. 27.
[38] *Ibid.*

different direction in relation to responding to digital power structures.

The bank example is incorrect in portraying individual employees as the ones with agency and the bank as a structure that enables this agency. It is incorrect because we actually do make banks accountable *as banks*. We do this through law by designating them as legal persons[39] and regulating them. Corporations are another example – they are social organizations granted legal personhood and so become agents through law.

In various ways Postema acknowledges the fact that agents can be artificial persons. For example, the 'new Leviathans' he targets are corporations and in an earlier discussion he recognizes that power-wielders can be nation-states, international organizations, and large employers.[40] However, there is a deeper lesson here for how we conceive of law's distinctive instrumentalities and how they can be enlisted to constrain digital power. The example of legal personhood highlights the ways in which law can *create* social structures. The legal personhood of entities like banks and corporations solves a social coordination problem by creating a new kind of agent who is recognized as acting in the world even though in fact it acts through individual human persons. Law can constitute social structures. To be clear, I am not suggesting that legal personhood is a solution to the problems of digital power. What I am suggesting is that we expand our understanding of the legal toolbox available to respond to digital power to include the ways in which law creates (social, economic, and technical) structures and thereby restructures our landscape of agency, accountability, and power.

Postema makes many comments about the role of law in the constitution of social and political power and how this constitutive function is different from the 'positive, normative, deliberative, and rights-defining dimensions of law'.[41] However, the focus of his discussions of this constitutive role is on *public* governing power and how there can be no legitimate governing power outside of that ordained by law.[42] He contrasts this with power exercised by private actors, where whatever is not prohibited is legally permitted. What

[39] See, e.g. Canada' Bank Act, SC 1991, c 46, s. 15.

[40] Law's Rule at p. 27.

[41] *Ibid.* at p. 44.

[42] *Ibid.* at p. 47.

this distinction leaves out are two considerations that are of crucial importance to thinking about digital power. The first is that private power is often constituted by law. This is the lesson of artificial persons, where law creates new forms of agency. But this is also true of many of the legal tools of private ordering, which creates the extension of agency by enabling activities that would not otherwise be possible. Postema acknowledges this to some extent in his brief discussion of legal formalities.[43] The second consideration is that law also constitutes forms of private power that can act as bulwarks against state power – many have defended private law in these terms, in particular private property.[44] Apart from private law, legal forms such as corporations and trusts have allowed for the creation of the civil society institutions that Postema argues are essential to fidelity.[45]

Because the lessons of law's role in prospectively protecting against the abuse of power 'through constituting and distributing power'[46] are not brought to bear on the problems of digital power, we are left with an impoverished legal toolkit in relation to digital power. The focus on Postema's chapter on digital power is on how law might constrain power-wielding rather than how law might help to constitute it. How, then, might we reclaim the potential of law's constitutive role? When Postema discusses the distinction between public and private actors I just pointed to, he argues that the distinction rests on the moral distinction between natural and artificial persons. Natural persons 'have moral standing independent of the law' whereas legally constituted persons are 'creatures and functionaries of the law'. He has in mind here 'officials' rather than private corporations, as corporations are not functionaries of the law. Nonetheless, there is also no reason to think that they should have equal *moral* standing as ordinary citizens. We might therefore say that digital power should only be wielded where permitted and

[43] *Ibid.* at p. 41.

[44] Richard Epstein, Design for Liberty: Private Property, Public Administration, and the Rule of Law (2011); T.R.S. Allan, The Sovereignty of Law: Freedom, Constitution and Common Law (Cambridge: Harvard University Press, 2013). For an alternative reading of the relationships between property and the rule of law see Jeremy Waldron, The Rule of Law and the Measure of Property (Cambridge: Cambridge University Press, 2012); Lisa M. Austin, ''Property and the Rule of Law'', Legal Theory 20(2) (2014): pp. 79–105.

[45] Postema acknowledges that ''[t]he law plays a crucial role in empowering, sustaining, and protecting these institutions and practices.'' (Law's Rule at p. 124.)

[46] *Ibid. at* p. 47.

authorized by law. This is not wildly novel. Data protection laws like the GDPR require that all data processing of personal data be 'authorized' – a requirement that does not apply to natural persons engaged in personal or household activities.[47] This is not an endorsement of the GDPR as a blueprint for managing digital power, for it is limited in a number of ways. My point is simply that the idea that all data flows require legal authority is one that already exists in some jurisdictions for some kinds of data flows. One type of rule-of-law response to digital power structures is therefore to look more critically at the ways in which law can legitimize and authorize data flows as a way of structuring social and political power.

Another type of rule-of-law response to digital power structures is to think more critically about the forms of social ordering that can act as a bulwark against digital power and how the law can be used to constitute those forms. For example, there is a growing literature about a range of data intermediaries that can facilitate data-sharing in ways that enable socially beneficial uses but that intervene in some way in the current practices of data monopolies.[48] Towards the end of his chapter on digital power, Postema endorses the general features of Aziz Huq's proposal of a public trust framework for data[49] and I would put Huq's work in this basket of proposals. According to Huq, we could create public trusts that would be managed for the public, providing constraints on private sector uses of data. It would, in turn, be subject to both democratic and judicial oversight. Postema endorses this proposal because it provides an example of how we can utilize the 'recognizable' tools in the traditional rule-of-law toolkit of 'justifying, authorizing, and enabling a government agency to define public norms' while providing formal and informal modes of accountability. I think that this misses the more radical nature of this growing body of (quite varied) proposals. Their importance lies in attention to the need for the creation of new social structures and modes of collective governance, even if they draw some of the

[47] See Article 6 of the EU General Data Protection Regulation (GDPR): Regulation (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[48] For a brief overview, see Lisa M. Austin and David Lie, "Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust", Surveillance & Society 19(2) (2021): 255–261.

[49] Law's Rule at pp. 288ff.

inspiration for these new structures from existing legal models.[50] In other words, what we need is the restructuring of our social and technical infrastructure that makes the exercise of digital power possible and not (only) the application of a traditional legal toolkit for constraining the exercise of digital power.

Even once we turn from law's role in constituting digital power and focus on law's role in constraining digital power, we need to get past an emphasis on human agency and ask what it means to hold s*ocio-technical systems* accountable. Let me point to three reasons for why this is so. First, we should be cautious about strategies for addressing power that default to an emphasis on human agency. The digital sphere is not one of agents and systems but socio-technical systems where determining the role of human agency and responsibility is notoriously complex. For example, Elish cautions us about creating what she calls 'moral crumple zones', which misattribute responsibility to human agents who act within complex technological systems:

> Just as the crumple zone in a care is designed to absorb the force of impact in a crash, the human in a highly complex and automated system may become simply a component – accidentally or intentionally – that bears the brunt of the moral and legal responsibilities when the overall system malfunctions. While the crumple zone in a car is meant to protect the human driver, the moral crumple zone protects the integrity of the technological system, at the expense of the nearest human operator.[51]

This caution is also applicable to proposals that seek to ensure a role for human agency within complex systems – such as 'human-in-the-loop' proposals for AI, or even transparency proposals that are meant to enable human oversight.[52]

Second, it is possible that we need to recognize new forms of agency other than human agency or fictional agency like the legal personhood of corporations. For example, Floridi points to advances in generative AI models – such as ChatGPT – as evidence that perhaps we need a new model of agency that can include artificial systems. He argues that generative models like ChatGPT represent 'a form of agency never seen before, because it is successful and can

[50] "Data Trusts", supra note 48, criticizes using the tools of private ordering to create a new data trust structure.

[51] Madeleine Clare Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction", Engaging Science, Technology, and Society 5 (2019): pp. 40–60 at p. 41.

[52] GDPR, *supra* note 47 at Article 22.

'learn' and improve its behaviour without having to be intelligent to do so'.[53]

Third, many aspects of our socio-technical systems function as infrastructure rather than discreet tools meant for discreet tasks. We can point to the ways in which such infrastructures create affordances that make power-wielding more or less likely and yet still think that this remains a separate question from the wielding of power in Postema's sense. But a focus on these affordances could lead to a different kind of standard-setting than Postema suggests. He points to the need for standards for the exercise of power whereas what we also need are standards that require digital infrastructure to be built in a manner that constrains rather than enables the exercise of digital power.[54]

But it is also not clear that the best intervention is to create public standards regarding the *ex ante* creation of the system. As Kingsbury and Maisy argue, the effects of infrastructures can be intentional or unintentional and are 'dynamic in the way a society or an ecosystem is'.[55] They 'create, shape, or prevent' the emergence of different types of social relations. What this calls for is attention to infrastructural publics and infrastructural governance.[56] Kingsbury and Maisy write:

> For the infrastructural public to be able to act within (or bear responsibility within) a legal system, it must have some proxy existence as a relevant legal public. This can be accomplished by numerous means, including formal organization of the infrastructural public; ad hoc recognition, for instance, in a legal class action; overlapped recognition, as when the right of an indigenous people to prior consultation or consent becomes a means of voice on infrastructure; or a kind of surrogate representation, where a court allows certain persons to speak for a nonpresent public.[57]

This is not an exhaustive list, and it does not address the specific problems of digital infrastructure. However, what we can see here is a shift away from a focus on agents who create infrastructure to its public governance, where 'public' refers the heterogeneous groups subject to their configuration of power relations.

[53] Floridi ''AI as Agency Without Intelligence: on ChatGPT, Large Language Models, and Other Generative Models'', Philosophy & Technology 36(15) (2023), https://doi.org/10.1007/s13347-023-00621-y.

[54] For some examples along these lines, although more about rights than the rule of law, see Julie Cohen, ''Affording Fundamental Rights: A Provocation Inspired by Mireille Hilldebrandt'', (2017) 4:1 Critical Analysis of Law 78.

[55] B Kingsbury and N Maisley, ''Infrastructures and Laws: Publics and Publicness'', (2021) 17 Annual Review of Law and Social Science 17(1) (2021): pp. 353–373, at p. 356.

[56] *Ibid.*

[57] *Ibid.* at pp. 364–365.

B. The Erosion of Informal Constraints

There is an additional dimension to the rule of law challenge in the data realm, one that is not about the wielding of digital power but about the erosion of sources of informal constraint on that power. Postema's account highlights some of this erosion in the digital sphere, especially in relation to the public sphere. However, Postema focuses on this erosion through the manipulative practices of digital platforms and their effects on fidelity. I agree with Postema's concerns but I think that the challenge to fidelity is a more basic and structural challenge. The use of digital technologies can shrink the degree to which formal systems of agency and accountability are open to informal constraints. This happens in specific ways and not just through the general undermining of an ethos of fidelity. Understanding this erosion is important if we are to design new systems of oversight.

Let me illustrate what I mean by returning to the bank example. In the example of the bank, we might say that to the extent that the 'bank' acts, it does so through its employees. I want to call this 'distributed human agency' because despite the bank's legal personhood what we have on the ground are multiple human agents who must be coordinated in some fashion according to internal bank norms and directives. Because of this distributed human agency, the bank is a social structure that is open to external social norms that affect the decision-making of these human agents. These social norms can exert their influence across a range of banking decisions from the tailoring of internal norms to local needs and unforeseen contexts to employee disobedience and whistleblowing. In contrast, in the data sphere we see significant automation and what this can look like is the reduction of distributed human agency. The coordination problem is solved through technology, increasing instrumental effectiveness (and power) while no longer being open to external social norms. Automation removes – or significantly lessens – informal mechanisms of constraint. The concern, in a nutshell, is that the opportunities for the kind of sociality contemplated by the principle of fidelity is shrinking in the digital realm as distributed human agency shrinks.

Let me add a few more examples, and layers, to the challenge. Suppose that the police are investigating a particular person and this

person was thought to have been in the vicinity of a particular neighbourhood on a particular day. The police can ask questions of people in the neighbourhood, and perhaps show them a photo of the person of interest, in order to see if anyone saw the individual and has further information. This is simple enough. Now consider the difference between that and a scenario from the digital realm. Take the facts of the Supreme Court of Canada case *R v. Spencer*, where the police asked a telecommunications provider for the subscriber information associated with a particular IP address known to have been used to download child porn.[58] The Supreme Court held that the police needed a warrant to do this. The Court also stated that asking the telecom for subscriber information was qualitatively different from routine police questioning of potential witnesses – without providing reasons as to why this was the case. As I have outlined in more detail elsewhere, I think that there are two key differences.[59] One difference is that in the first example the agency of others is distributed across multiple people in a neighbourhood whereas in the second example agency is concentrated in the telecom. This agency involves both determining whether to participate in holding a potential perpetrator to account through cooperating with the police as well as whether the police are trustworthy in their requests. These decisions are not just about holding community members to account, but also the police. A second difference is that in the first example the police investigation takes place in public and in the second example it is known only to the telecom. These two features of the first example – distributed agency and public transparency – allow for the kind of community accountability-holding practices that Postema discusses in his account of fidelity. The features of the second example – concentrated agency and opacity – mean that only the telecom has the ability to engage in accountability-holding. This potentially augments police power by removing practical constraints on its exercise and increases the power of telecoms by making their users vulnerable to actions that neither they nor the data regulators can see.

This analysis allows us to see that the reason for imposing additional constraints on the police when they seek the information from

[58] R v. Spencer, 2014 SCC 43.

[59] Lisa M. Austin, ''Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints'', Theoretical Inquiries in Law 17(2) (2016): pp. 451–485.

the telecom rather than neighbourhood witnesses (i.e. requiring a warrant) is not necessarily because the privacy interest is different but because a set of informal constraints has been removed and new constraints need to be put into place. Postema's account of fidelity can help us to understand this as a rule of law concern.[60] This example therefore shows how law can respond through replacing constraints that are otherwise eroded in the digital realm because of the loss of distributed agency. But notice that the solution here – court supervision of the police – does not re-enable informal practices (community participation) but displaces them into the realm of formal practices (judicial oversight). We should not be sanguine about these formal practices. As police reliance on data becomes more complex, court oversight becomes practically less effective and the decisions of digital agents like telecoms become more important.

It is not just the structural shrinking of the opportunities for community agency in accountability practices that is at stake here. Also important is the loss of community participation in social norm creation. In addition to the informal practices of accountability-holding just discussed, the formal law is often open to the influence social norms, taking them up in a variety of ways and contexts.[61] Consider again the example of the police having to go into a community to ask potential witnesses to come forward. If the police require community cooperation in order to engage in their investigations then they will require community trust. There is a reciprocity here that is not just about the community determining whether some set of formal norms have been met but is about the ongoing co-creation of practical norms of engagement. Properly reclaiming this role requires creating modes of accountability that can provide space for community participation.

Postema discusses the importance of such community participation in a few places, particularly in relation to practices that allow for the contestation of norms. He also, as already alluded to, points to the need for public spaces for mutual engagement and the development of social trust. What I am pointing to here is the need to

[60] Search and seizure jurisprudence has always had an underlying concern for the rule of law. See Thomas Y. Davies, ''Recovering the Original Fourth Amendment'', Michigan Law Review 98(3) (1999): pp. 547–750; Lisa M. Austin, ''Getting Past Privacy?: Surveillance, the Charter, and the Rule of Law'', Canadian Journal of Law and Society 27(3) (2012): pp. 381–398.

[61] See Law's Rule at pp. 157–160 for a discussion of norms.

create new models of oversight that can engage the multiple publics in specific practices of accountability holding. These publics would not be defined by public *space* or political boundaries but by being subject to another's governing power – public or private.

C. The Limits of Law's Distinctive Toolkit

Transparency is an important pre-condition for the rule of law. Opacity hampers both the community-based practices at the heart of fidelity and the official practices of regulators: digital power cannot be made accountable if its practices are effectively invisible to accountability-holders. Postema's discussion of transparency in the digital realm focuses on algorithmic transparency. Algorithmic transparency and explainability are important but fairly specific concerns that arise from Postema's focus on data giants and their manipulative practices, practices that increasingly rely upon AI. I want to point to a more systemic concern regarding transparency in the digital sphere – the lack of transparency regarding data flows – and show why this highlights some of the limits of law's distinctive toolkit.

This problem already arose in the lawful access example of the previous section, where the police practice of asking data giants for subscriber information is not visible to the general public. Such practices can be made visible if an individual is charged with a crime and then challenges the practice in open court, or if a data protection regulator chooses to use their investigative powers to audit them. They can also be made visible through the practice of 'transparency reports' where telecoms provide aggregate statistics about the requests they receive. Such reports provide weak transparency due to their general nature and the fact that they are an example of self-reporting. Data flows can also be made visible through privacy policies, although there are few people who see these policies as successful examples of transparency practices.

Let me add another layer to the transparency challenge, which is the role of third parties in the data ecosystem. Dominant regulatory models, like data protection laws such as the GDPR, focus on the relationship between an individual and an organization. However, that organization might use third parties to assist in their own pro-

cessing of data and they might, for various reasons, disclose data to third parties to be processed for the purposes of those third parties. For example, the Cambridge Analytica scandal concerned the way in which Cambridge researcher Aleksandr Kogan obtained access to Facebook user data for the purposes of his app 'thisisyourdigitallife', not for Facebook's purposes. Facebook facilitated this kind of access in order to create a vibrant third-party app ecosystem. The problem was that Kogan then shared this data with Cambridge Analytica in violation of Facebook's platform policies[62], which explicitly prohibited use for commercial purposes.

Regulators in the UK, the US, and Canada all concluded that Facebook had failed to properly obtain consent from its users for these disclosures and also that it had failed to put in place adequate safeguards to ensure that the third party app developers who were granted access actually adhered to Facebook's policies.[63] I want to focus on the 'safeguards' issue for the purposes of my discussion here, rather than the consent question. The evidence is that Facebook did not know that Kogan has disclosed user information to Cambridge Analytica until an article was published in the Guardian, at which point it terminated Kogan's access and began its own investigation.[64] What the regulators held, however, was that Facebook should have done more to proactively monitor adherence to its policies. The Canadian regulators argued that it is Facebook who 'knows precisely which apps get what data and when, and has the unique ability to monitor apps proactively to protect users before any unauthorized disclosure occurs'.[65] The FTC order requires that Facebook have its third party app developers self-certify that they are following its policies but also that Facebook monitor for compliance – monitoring that should include 'ongoing manual reviews and

[62] Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian, March 17, 2018.

[63] Information Commissioner's Office, Facebook Ireland Ltd. Monetary Penalty Notice (24 Oct 2018) (ICO Penalty Notice); Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, PIPEDA Report of Findings #2019-002 (OPC Joint Investigation). United States v. Facebook, Inc., No. 19-cv-2184 (DDC, 24 July 2019) at paras. 118-119 [hereinafter FTC Settlement Order 2019]. The language of "safeguards" is from data protection law. In the US, the FTC framed the obligation to monitor for compliance as part of Facebook's obligation to have a "privacy program".

[64] ICO Penalty Notice, *supra* note 63 at para. 43.

[65] OPC Joint Investigation, *supra* note 63 at para. 158

automated scans, and regular assessments, audits, or technical and operational testing[.]'[66]

By placing a strong obligation on Facebook to use technical safeguards and not just contractual safeguards, as well as to proactively monitor compliance, the data regulators highlight for us the new reality that maintaining legal compliance in the digital sphere will require us to go beyond our existing legal tools and embrace new technological tools. In particular, it points to the need for automating policy analysis and combining this with auditing practices to determine whether practices accord with policies. In some ways, this is not surprising. If I am right in arguing previously that we need to think in terms of how to ensure the accountability of socio-technical systems, then we should not think that this can be done either by focusing on the tools we have developed to manage social systems or the tools we have developed to manage technical systems.

Even if this is so, several problems remain. The first is placing the obligation on data giants to engage in the monitoring of third parties.[67] While understandable for the reasons offered by the regulators, this places these data giants in charge of ensuring accountability for data flows while otherwise maintaining opacity in the data ecosystem. Users, civil society, and regulators all continue to remain in the dark with their own role in accountability-holding compromised. The second problem is that creating these technical tools is very challenging and will likely require the creation of legal obligations to create socio-technical systems in ways that facilitate such auditing. We need to engineer for accountability. The third problem is that when we engineer for accountability there is a serious question of whether we are still within the realm of legal accountability and not something else.

This last problem raises the concerns that Postema begins to address in his chapter on the use of AI in law. His focus is on proposals for 'artificial legal intelligence' that can *replace* legal officials.[68] Postema's main argument against AI as a replacement for law is that although AI might effectively constrain governing power, it

[66] FTC Settlement Order 2019, *supra* note 63 at VII. E. c.

[67] For a general discussion of this trend, see Rory Loo, ''The New Gatekeepers: Private Firms as Public Enforcers'', (2020) 106 Virginia Law Review 106(2) (2020): pp. 467–522.

[68] Law's Rule at p. 294.

does so in a manner that eschews law's distinctive mode of ordering. Instead of guiding behaviour, Postema argues, AI technologies 'channel and goad it'.[69] Legal reasoning is different from AI's mode of reasoning, for it is practical, involves judgment, fundamentally relies upon analogies, and has a moral dimension.[70] The problem with this analysis is that it leaves us with few resources with which to understand how AI might be used as a tool of compliance within a legal system, rather than as a replacement to it.

We can think of an analogy to this problem if we think about the role of police in a polity subject to the rule of law. As Postema argues, the rule of law does not require the use of coercive force and 'law and order' accounts of the rule of law are seriously misguided.[71] In an earlier article, Postema contrasts a model of accountability 'fit for law' with the exercise of coercive power by the police. He argues that '[a]ccountability that focuses solely on providing external incentives (especially coercive incentives) for compliance leaves out of the picture the crucial discursive element of law and fails to appreciate and make use of the full range of the offices of the law'.[72] At the same time, it is not difficult to imagine that in many practical contexts a state without recourse to police enforcement of the law will be a state where law fails to rule and private violence takes hold. The point is not to transform coercive police power into non-coercive power but to use law to constitute and constrain this coercive power. We need to accomplish something similar with AI and other tools of automation – to recognize that this technology is not a part of law's distinctive mode of ordering but that it can nonetheless be constituted and constrained by law and become an important practical component in maintaining the rule of law.

IV. CONCLUSION

In *Law's Rule*, Gerald Postema provides a robust theoretical framework that technology scholars can use to analyze power and the possibility of the rule of law in the digital world. He articulates how the rule of law can be concerned with private power, and not just

[69] *Ibid.* at p. 298.

[70] *Ibid.* at pp. 299–300.

[71] *Ibid.* at p. 54.

[72] Gerald Postema, '"Trust, Distrust and the Rule of Law"', in P.B. Miller and M. Harding (eds,), Fiduciaries and Trust (Cambridge: Cambridge University Press, 2020), pp. 242–272 at p. 247.

public power. He also articulates why the rule of law is not just concerned with the exercise of power but also the possibility of its exercise and the structures that enable its exercise. His emphasis on the ethos of fidelity also provides a powerful tool for analysis of how the rule of law of law may be degraded in the digital era through the erosion of the informal institutions and practices needed to sustain the rule of law.

As helpful as this framework is, it only takes us part of the way to grappling with digital power from a rule-of-law perspective. I have argued that such an agenda requires more engagement with what it means for the rule of law to concern itself with the structures that enable private digital power instead of the wielders of digital power, that the erosion of fidelity is not just a matter of the manipulative practices of platforms but also occurs through the erosion of what I have called distributed human agency, and that addressing sociotechnical systems might require rethinking law's distinctive instrumentalities in order to embrace the use of digital technologies to increase transparency and compliance.

ACKNOWLEDGEMENTS

Gerald J. Postema, Law's Rule: The Nature, Value, and Viability of the Rule of Law (Oxford and New York: Oxford University Press, 2022) [Hereinafter Law's Rule]. I would like to thank Gerald Postema for his generous engagement with the arguments of this paper. I would also like to thank the other participants in this symposium for their many helpful interventions and for the insightful comments of my reviewer. All remaining errors are mine.

University of Toronto Faculty of Law, 78 Queen's Park, Toronto, ON, M5S 2C5, Canada
E-mail: lisa.austin@utoronto.ca