Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2019: 1–15

DOI: 10.1177/2053951719829773
journals.sagepub.com/home/bds
SAGE

Logged out: Ownership, exclusion and public value in the digital data and information commons

Barbara Prainsack

Abstract

In recent years, critical scholarship has drawn attention to increasing power differentials between corporations that use data and people whose data is used. A growing number of scholars see digital data and information commons as a way to counteract this asymmetry. In this paper I raise two concerns with this argument: First, because digital data and information can be in more than one place at once, governance models for physical common-pool resources cannot be easily transposed to digital commons. Second, not all data and information commons are suitable to address power differentials. In order to create digital commons that effectively address power asymmetries we must pay more systematic attention to the issue of exclusion from digital data and information commons. Why and how digital data and information commons exclude, and what the consequences of such exclusion are, decide whether commons can change power asymmetries or whether they are more likely to perpetuate them.

Keywords

Digital data, digital information, commons, exclusion, governance

This article is a part of special theme on Health Data Ecosystem. To see a full list of all articles in this special theme, please click here: https://journals.sagepub.com/page/bds/collections/health_data_ecosystem.

The iLeviathan: Trading freedom for utility

As a concept, 'Big Data' started to become an object of attention and concern around the start of the new millennium. Enabled by new technological capabilities to create, store and analyse digital data at greater volume, velocity, variety and value[1] the phenomenon of Big Data fuelled the imagination of many. It was hoped to help tackle some of the most pressing societal challenges: Fight crime, prevent disease and offer novel insights into the ways in which we think and act in the world. With time, some of the less rosy sides of practices reliant on big datasets and Big Data epistemologies became apparent (e.g., Mittelstadt and Floridi, 2016): Data-driven crime prevention, for example, requires exposing large numbers of people to predictive policing (e.g., Perry, 2013), and 'personalised' disease prevention means that healthy people have to submit to extensive surveillance to create the datasets that allow personalisation in the first place (Prainsack, 2017a). In addition, it became apparent that those entities that already had large datasets of many people became so powerful that they could eliminate their own competition, and at the same time *de facto* set the rules for data use (e.g., Andrejevic, 2014; Pasquale, 2017; see also van Dijck, 2014; Zuboff, 2015). GAFA – an acronym combining the names of

Department of Political Science, University of Vienna, Universitaetsstrasse, Vienna, Austria; Department of Global Health & Social Medicine, King's College London, London, UK

Corresponding author:
Barbara Prainsack, Department of Political Science, University of Vienna, Universitaetsstrasse 7, 1010 Wien/Vienna, Austria.
Email: barbara.prainsack@univie.ac.at

some of the largest consumer tech companies, Google, Apple, Facebook and Amazon – have become what I call the *iLeviathan*, the ruler of a new commonwealth where people trade freedom for utility. Unlike with Hobbes' Leviathan, the freedom people trade is no longer their 'natural freedom' to do to others as they please, but it is the freedom to control what aspects of their bodies and lives are captured by digital data, how to use this data, and for what purposes and benefits. The utility that people obtain from the new Leviathan is no longer the protection of their life and their property, but the possibility to purchase or exchange services and goods faster and more conveniently, or to communicate with others across the globe in real time. Increasingly, the iLeviathan also demands that people trade privacy and freedom from surveillance for access to services provided by public authorities (Prainsack, 2019). The latter happens, for instance, when people are required to use services by Google, Facebook, or their likes in order to book a doctor's appointment or communicate with a school (see also Foer, 2017). For many of us, it also happens when access to a public service requires email.[2]

This situation has garnered reactions by activists, scholars and policy makers. Reactions can be grouped in two main approaches, depending on where the focus of their concern lies: On the one side are those who want individual citizens to have more effective control over their own data. I call this the *Individual Control* approach (Table 1). It comprises (a) those who deem property rights to be the most, or even the only, effective way to protect personal data, as well as (b) some of those who see personal information as an inalienable possession of people. The latter group reject the idea that personal data should be protected by property rights and prefer it to be protected via human rights such as privacy, whereby privacy is understood to be an individual, rather than a collective right (see Table 1). Solutions put forward by scholars in the *Individual Control* group include the granting of individual property rights to personal data (see below), or the implementation of ever more granular ways of informing and consenting data subjects (e.g., Bunnik et al., 2013; Kaye et al., 2015). The spirit of the new European Union General Data Protection Regulation (GDPR) tacks mostly to an *Individual Control* approach in the sense that it gives data subjects more rights to control their personal data – to the extent that some might see it as granting quasi-property rights.[3]

The second approach – which I call the *Collective Control* approach – comprises of authors who emphasise that increasing individual-level control over personal data is a necessary but insufficient way to address the overarching power of multinational companies and other data capitalists. Scholars within the *Collective Control* group are diverse in their assessment of the benefits and dangers of increasing individual-level control.[4] What they all have in common, however, is that they foreground the use of data for the public good.[5] Many of them see the creation of digital data

Table 1. Main strands of arguments about how to address the asymmetry of power between data subjects and corporate data users.

Strategy	Authors in this group conceive personal data and information as:
Strengthening individual-level control (*Individual Control group*)	(a) individual property protected by property rights OR (b) inalienable individual possessions protected by individual civil rights
Strengthening collective public control, increasing public value (*Collective Control group*)	inalienable *personal* possessions that have an individual *and* a social component; protected by individual civil rights and by collective public ways of control and responsibility AND/OR public value of personal data and information should be enhanced (e.g., data philanthropy, data commons; see also Taylor, 2016)

Source: Author.

and information commons as the best way to do this, often because of the emphasis that commons place on collective ownership and control. Some authors also see the creation of commons explicitly as a way to resist 'the prevailing capitalist economy' (Birkinbine, 2018:[6] 291; Hess, 2008; De Peuter and Dyer-Whiteford, 2010; for overviews see Hess, 2008;[7] Purtova, 2017a).

In the following section, I will scrutinise the claim made by some authors within the *Collective Control* group that digital data and information commons can help to address power asymmetries between data givers and data takers. Despite the frequent use of terms such as 'digital commons' and 'data commons' in the literature, I argue that the question of what kind of commons frameworks are applicable to digital data and information, if any, has not been answered with sufficient clarity. In the subsequent part of the paper I will discuss another aspect that has not received enough systematic attention in this context, namely the topic of exclusion. I argue that collective measures to address power asymmetries in our societies need to pay explicit and systematic attention to categories, practices and effects of exclusion. I end with an overview of what governance frameworks applicable to digital data and information commons need to consider if they seek to effectively tackle inequalities. If they fail to do this, they risk that they are most useful to those who are already privileged and powerful.

What are commons, and how can they be governed?

Throughout different times and places, the term 'commons' has signified a broad range of phenomena ranging from communal agricultural land, town squares, campus dining halls, or non-titled citizens (Hess and Ostrom, 2003: 115). As Charlotte Hess and Elinor Ostrom observed in the early 2000s, in legal scholarship, the commons have often been used synonymously with the public domain (Hess and Ostrom, 2003: 114; see also De Peuter and Dyer-Whiteford, 2010; Litman, 1990) or the non-profit sector (Lohmann, 1992). This has made the commons a symbol of opposition to 'private property' and commercial interest. This view is problematic for two reasons: The first is that it implies a false dichotomy between private resources on the one hand, and shared or 'common' resources on the other. Shared resources are often governed by private property regimes. Second, the conflation of commons and 'open access regimes' – namely resources that are not owned by anyone – obscure the fact that the very possibility to govern a resource in a fair and equitable way requires that *someone* owns it. If nobody owns it, then anyone can use the resource as she or he pleases, often with the result that powerful entities can make better use of the resource than those with less power. The enclosure of land and the resulting structure of land ownership in many countries illustrate this.

But what type of property regime is most appropriate for commons? Following Bromley (1990) I distinguish between four main property regimes, depending the entity that is authorised to decide over the fate of the thing that is owned (Table 2): The first is *state property*, where ownership and control rest with the state, which means that state authorities decide about access and use rights.[8] The second is *individual property*, owned by individual (natural or legal) persons. The third type is *common property*, where property rights are jointly held by a group who can exclude all others from accessing, governing and using the object or

Table 2. Types of property regimes (adjusted and expanded from Bromley, 1990).

	Property regime type	Examples	Public/private property	Can people be excluded from access/use/governance?
A	State property regime	National forests, state-owned casinos	public	Yes – e.g., non-residents, minors, etc.
B	Individual property regime (can be held by more than one person, e.g., spouses)	Homes and personal property	private	Yes
C	Common property regime (*res communis*)	shared gardens	private	Yes – typically those who are not members of the group that owns the object/resource
D	Open access regime (*res nullius*)	the open sea, air	n/a	No

resource. The fourth type is *open access* regimes[9] where no property rights to an object or resource have been recognised.

Many of the resources that have traditionally been associated with commons are governed by state or common property regimes. Examples include community grasslands, forests, or agricultural cooperatives. Grassland and forest commons could be owned by the state, for example, but be governed by local communities.[10] Agricultural cooperatives are jointly owned by the people running them. As such they comprise public and private ownership arrangements respectively. The one regime that seems unsuitable for effective commons governance is open access (*res nullius*).

Also the commons scholar and Nobel laureate Elinor Ostrom and her collaborators saw the right and the possibility to exclude people from the commons as key to the governance of commons.[11] This stands in stark contrast to scholars who see commons as resources owned by nobody.[12] One of these authors is Lawrence Lessig, who defined the commons as 'a resource that anyone can draw upon without the permission of someone else' (Lessig, 2009: 35. See also Lessig, 2001). Similarly, for Michael Heller, the right of people not to be excluded plays such an important role in defining the commons that he coined the term of the 'anticommons' for property regimes in which (multiple) owners can exclude others.[13]

Also the commons 'pessimists' – namely those authors who see commons as vulnerable to overuse and exploitation (Hardin, 1968; see also Feeny et al., 1990) – typically assume commons to be governed by open access regimes so that nobody can be excluded from them. In contrast to those who consider the impossibility to exclude a desirable feature, commons pessimists see this as a problem.[14] If anyone can use the resource, they argue, then nobody has an incentive to protect and invest in the resource either (for a discussion of this point see Hess and Ostrom, 2003:121). Hardin's classical case of a shared grazing ground that is depleted because it is overused by self-interested cattle owners, however, has been criticised for confusing commons with a rule-less 'no-man's-land' (Bollier, 2014: 24) populated by people without concern for others or for the resource as such.

Many commons scholars conceptualise commons as consisting of a material resource in combination with the rules and communities governing it. The material resource can further be differentiated into stock units, which make up the core resource, and fringe units, which can be consumed without damaging the stock. The typical resource that Ostrom and her collaborators analysed in the first decades of commons scholarship were fisheries, farmland and other resources that they called *common-pool resources*. The essential characteristics of common-pool resources are the aforementioned possibility to exclude, and also that they are 'subtractable'. This means that the degree to which a person uses a resource subtracts from the potential use of others. Good governance of common-pool resources thus needs to avoid that mis- and overuse destroys the core resource, and to ensure that those using it – so-called appropriators – maintain and care for the commons.

Based on her analysis of actual cases of common-pool resource uses, Ostrom distilled 'design principles' for the governance of common-pool resources (which many authors use synonymously with 'commons'). In the following I use commons as a generic term for a jointly owned and governed resource, whereas I use the term common-pool resource in the way that Ostrom and her collaborators defined it. To start with, to be open to the possibility of good governance, a commons needs to have clearly defined boundaries – both in terms of the physical resource and regarding the owners of the commons. In other words, it needs to be clear, for example, where a grazing ground for sheep begins and ends, and who the members of such a commons are. Second, governance rules need to be appropriate to local conditions, e.g., to the ecological conditions that the resource is part of. There also need to be mechanisms for inclusive collective decision making, and processes need to be in place for the monitoring of appropriators. In case of rule violations, graduated sanctions need to be applied, and conflict resolutions must be fast and inexpensive. The self-governance of the commons needs to be recognised by the political and legal system that the commons is surrounded by, so that nobody can interfere with what the members of the commons decide. Last but not least, governance should be organised in layers of nested enterprises (Ostrom, 1990; see also Agrawal, 2002).

Given that Ostrom has shown how common-pool resources can be governed without damaging or destroying them, can we apply these design principles to digital data and information commons?

Can there be data and information commons? The challenge of data multiplicity

For over a decade, authors have called for the creation of commons in order to collectivise access to, and the benefits of, digital data and information (e.g., Benkler, 2002; 2004; Hess, 2008). But can we think of digital data and information as common-pool resources in Ostrom's sense? Can digital data and information

form a commons to which Ostrom's design rules could be applied? I argue that we cannot, as I will lay out in the next section.

The multiplicity of digital data and information

There is no doubt that digital data and information require materiality to exist, including the human, natural and artefactual tools and infrastructures that curate, store and process them (see also Leonelli 2016). But unlike letters, numbers or illustrations on a piece of paper, a digital datum does not necessarily correspond with only one specific material unit where it 'sits'. The materiality of digital data is distributed in space and time. A patient's health data may have a specific 'place' on the hard drive in the hospital database where it is stored, but it 'moves' to wherever it is accessed from computers in different clinics or departments of these hospital, or the patient's own computer or mobile phone. Similarly, digital information in the cloud can be downloaded to several electronic devices in different parts of the world at the same time, and permanently reside on these devices. In contrast to data on paper that can also be torn up or burned or irreversibly destroyed by other means, digital data leaves traces even when they are deleted. In sum, digital data is *multiple* in that it can be in several places at the same time, and in that it can continue to exist in one place when it was removed from another.[15]

It is the multiple nature of digital data that renders the notion of control over data so complex. Regarding a paper file in the hospital cabinet locker containing patient data, we can establish with relative ease who has control of the file. The doctor, nurse or administrator, or other hospital staff decides who holds the keys to the cabinet, who can see the file, who may carry it out of the room, or who may even photocopy it. With digital data, establishing who has or could get access to the dataset, and who controls how it is used, is much more difficult. Given the crucial role that meaningful (collective) control plays in governance frameworks for commons, this raises the question to what extent these frameworks – and in particular, Ostrom's design principles – are applicable to digital data. A key aspect in this regard pertains to ownership: As noted, ownership (and, as some would argue, property rights) are a precondition for effective governance because only ownership enables parties to set rules and exclude those that would exploit the commons without contributing to it. But can we own, or even hold property rights, to something that is multiple, i.e., that exists in several places at the same time?

Owning digital information and data: Data and information commons

Legally, the answer is yes. Intellectual property rights entitle the holders to exclusive and enforceable control also over intellectual resources that are entirely non-material. All jurisdictions grant intellectual property rights in some form. But intellectual property rights are typically given to artistic or creative artefacts, such as inventions or artworks. The situation gets more complicated when what is at stake are not ideas, but instead personal data and information, namely – using an EU definition[16] – any information that relates to an identified or identifiable living individual. Law and theory put personal data and information in a separate category from other data and information as they are seen to have a particularly close connection with personhood. Personal data and information disclose things about us and our lives that we may want to keep confidential or even private, and that may harm us if they are known or used by others. For these reasons, most jurisdictions place restrictions on the collection and use of personal data. But there are crucial differences in *how* personal data is protected.

In Europe, the predominant view has been to see personal data and information as belonging to people in a moral sense, without being considered individual property in the legal sense. That is, personal data is not considered something that can be sold.[17] Instead, personal data and information are protected by privacy rights, which are 'an integral part of being a citizen' (Zwick and Dholakia, 2001: 218). In this view, personal data and information cannot be sold by those who possess them, and must not be violated by others.[18]

In the United States, debates about whether personal information should or could be viewed as property have been complex. Some might argue that the idea of property rights, understood – in William Blackstone's deliberately provocative description – as 'that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe' (Blackstone, 1979 [1765–1769]), are one of the foundations upon which American society was created. Others hold that this idea has never corresponded with actual law; moreover, throughout the 20th-century, the nature of property rights have been reconceptualised as a *bundle* of rights (Heller, 1998: 661–662; see also Rose, 1998) that could be held by different parties. These rights include the right of enjoyment, the right of disposition and the right of exclusion.

As Nadezhda Purtova argues, in U.S. discourse, the propertisation of personal information has served to address three goals: First, to overcome the shortcomings of U.S. data protection systems; second, to give people control over their personal information; and third, to provide incentives for companies to respect privacy (Purtova, 2009: 507–508). Some U.S. authors have argued that individual property rights are the only way to ensure information privacy (Murphy, 1996; discussed in Purtova, 2009). This is because there is no other way to ensure that people have meaningful and effective control over their data in a legally enforceable way.[19] Following this rationale, property rights to personal information could be seen to take on the additional role of addressing power asymmetries (Kang, 1998, discussed in Purtova, 2009).[20] Other authors, such as Jessica Litman, disagree with this stance, arguing that 'the raison d'être of property is alienability' (Litman, 2000: 1295). In this reading, property rights encourage transferring property rights instead of protecting them (see also Purtova, 2009). In other words, if we see personal information as an inalienable possession – that is, as something that we own in a moral sense but that we cannot give away – then property rights are unsuitable as a protective device. They are unsuitable because they encourage the very thing that the European approach deems morally inappropriate (and ontologically impossible), namely the transfer of exclusive rights to data.

I have proposed that digital data and information are different from traditional physical common-pool resources in that they are multiple, which makes it difficult to control them. The difficulty to effectively control the use of data in a genomic data repository is a case in point: This information multiplies fast as people download and share this information with others. Irrespective of whether we deem property rights or human rights regimes more appropriate to govern digital data and information, the effectiveness of either of these may be jeopardised because of how difficult it is to control digital data and information effectively. This, as I will show in the next section, also hinders the applicability of the design principles for the governance of common-pool resources to digital data and information commons.

Are the design principles for common-pool resources applicable to digital data and information commons?

As noted, Ostrom's design principles for common-pool resources start with the requirement that commons need to have clearly defined boundaries – both in terms of the physical resource and the owners of the commons. Despite the fact that also 'traditional' commons such as fisheries and grazing land also include intangible things, such as the practices and values that produce and reproduce the resource (see Benkler and Nissenbaum, 2006; Linebaugh, 2008), digital data and information are special in that they can be in several places at the same time, when no central control point exists that knows where they are located. This multiplicity of digital data and information makes it extremely difficult to meet the requirement of clear boundaries (see also Purtova, 2017a).[21]

It could be tempting to dismiss Ostrom's second design principle, namely that governance rules need to be appropriate to local conditions, by positing that digital data and information commons are global resources that have no specific local conditions. But this would be rash. As many authors have argued (e.g., Gitelman, 2013; Leonelli, 2016), the curation and use of digital data and information is always local insofar as it is dependent on the work of specific people, instruments, infrastructures that are in turn part of specific local configurations and contexts. At the same time, because of the multiplicity of digital data, these localities can be multiple for each data point. A digital commons comprising health and medical data from volunteers, for example, is local not only in the sense that clinical data was collected according to the rules and within the infrastructures of local healthcare systems, but also in the sense that the very biology of the person reflects the locality of the person. A person living in central London may suffer from respiratory problems due to pollution, or even bear the marks of epigenetic changes due to the bad air quality. In sum, digital data and information are local in so many respects that it is often not discernible how many and what kind of localities datasets are part of. This also relates to the previous point that digital data and information commons typically have no clearly defined boundaries. Thus, while matching governance rules to local conditions would be possible, in theory, in the context of digital data and information commons, because of the multiple locations of digital data and information and because of the distributed localities of who and what they represent, it would be particularly difficult to ensure that governance rules are well-matched to local conditions.

The third to sixth design principles – inclusive collective decision making, processes for monitoring appropriators, graduated sanctions in case of rule violations, and fast and inexpensive conflict

resolution – can be realised in digital data and information commons, as long as they are not governed by open access regimes (*res nullius*).

Design principles seven and eight would again be very difficult to realise with digital data and information commons irrespective of the property regime they are governed by. If it is not clear where the commons starts and ends, and who the members are, then it will be very difficult, if not impossible, to establish a self-governance system for the commons that is recognised by law. For the same reason would it also be hard to organise governance in layers of nested enterprises.

In summary, the assumption that digital data and information are (or can be treated analogous to) a physical common-pool resource and be governed by established principles designed for commons does not stand up to scrutiny. Although digital data and information clearly have material components, their materiality is of a very different kind than the physical resources that have been in the centre of commons scholarship. The multiplicity of digital data and information – the fact that they are distributed in time and space – also means that some of the key design principles developed for physical commons cannot be met.

While this means that we cannot answer questions about the governance of digital commons by referring to design principles developed for physical commons, this does not imply that digital data and information cannot be organised as commons at all. But it means that digital commons require specific governance frameworks, which is what I will turn next. I will argue that systematic attention to who and what is excluded from digital commons need to be a key concern in designing and governing digital commons, especially if we intend commons to counteract existing power asymmetries in our societies.

In- and exclusion in the data and information commons

Within scholarship on the commons, including the digital data and information commons specifically, there has been surprisingly little explicit discussion about the categories, processes and effects of exclusion. Part of the reason for this is the egalitarian rhetoric surrounding 'the Internet'. It suggests that web-based tools and platforms are instruments for democratisation and egalitarianism because in principle, everybody can use them. That this view of the Internet as a democratisation machine is unduly naïve has become widely accepted over the last years (Morozov, 2011; Taylor, 2014), and increasing attention has been paid to the extent to which the Internet in itself is made up of enclosures (Schiffman and Gupta, 2013). It would be wrong to assume, however, that the problem of exclusion can be solved by applying open access regimes to digital data and information from which nobody can be excluded. As noted, the risk of overuse and ultimately the destruction of the commons is highest when the resource is not owned by anybody. For many of those who see commons as a way to enhance public benefit and public value, the conclusion that commons should ideally be governed by *public (state)* property regimes is plausible. But even this conclusion would be too hasty: Inclusion and exclusion, and empowerment and disempowerment, have complex relationships to private and public property regimes. For example, as Lezaun and Montgomery (2015) noted, private property – for example in the form of intellectual property entitlements – can be conducive to wider inclusion if those with fewer rights and less power are actively invited to contribute to, share and use the resource. Correspondingly, the formally equal access for all citizens[22] that public property regimes typically offer can mean, in practice, that those who are already powerful can use public resources most effectively and against the interests of others. This is the case when free university education mostly benefits middle class students because fewer working class students go to university, or when rich and powerful land owners such as the British royal family claim millions in farming subsidies from the European Union (see also Taylor, 2014; Rose, 2003).

I argue that we should foreground the question of how public value and public benefit can be increased in digital commons arrangements in a way that is applicable to all type of property arrangements, including public and private ones. For this endeavour, practices, categories and effects of in- and exclusion are crucial. Paying more systematic attention to practices and categories of in- and exclusion in digital data and information commons helps us to distinguish between commons that have the potential to counteract structural asymmetries of power and those that do not.

Scrutinising the categories, processes and effects of exclusion

Jodi Dean used the notion of 'reflective solidarity' to draw attention to the need to critically reflect how and where we draw boundaries around communities, how we differentiate between 'us' and 'them'. Reflective solidarity 'refers to a mutual expectation of a responsible orientation to relationship' (Dean, 1996: 29) by which responsibility signifies that we are accountable for who

and how we exclude. Following Dean's call for reflective solidarity means that we need to make explicit the substantive values, norms and categories that make us recognise similarities and commonalities with some people and not others, and thus enact support for some rather than others. This does not mean that differences between people should be ignored or overcome, or that exclusion is always problematic: Seeing how and where we are different from others is a fundamental necessity of human and social life. Even the most 'radical' relational accounts of personhood do not negate the importance of some processes of othering. Similarly, excluding people from using something that is not of important value to them, or excluding them from using something that they can easily use elsewhere, is not problematic: If I exclude somebody from access to my garden this is ok if this person has her own garden down the street. It is more problematic when the person cannot afford to have her own garden, and when there are no communal gardens and parks within her reach. When we replace gardens with healthcare in this example, then exclusion becomes even more contentious. Exclusion is most problematic where it significantly and negatively affects fundamental human needs and interests, including healthcare, social services, education and transportation, and, as increasing numbers of people argue, also online connectivity.[23]

Much of the literature on digital data commons in the realm of health has assumed that the best way of going about this would be for people to actively and voluntarily opt for their data to be included to commons (e.g., Evans, 2016; Hafen et al., 2014; most of these proposals envisage data governed by common property regimes). I support this argument insofar as the governance mechanisms of commons can help to ensure that data and information are not used in ways that are likely to incur significant and undue harm to those whose data is included in these commons.[24]

Problems with such inclusive databases in the health domain arise (a) when people, whose data is in the database, do not have a say in the databases governance, even if they would like to, and (b) when no appropriate harm mitigation instruments exist. The former is exactly the problem that commons arrangements could successfully address, if they give all those who contribute to the commons the possibility to participate in its governance, and if collective governance mechanisms are transparent and accountable to all contributors. The latter issue, adequate harm mitigation instruments, requires new measures that we have started to lay out in a different publication (McMahon et al., 2019).

In sum, exclusion is not problematic in itself. When and how it is acceptable to exclude depends on the nature and function of the digital data commons, and from what contributors are excluded. At the same time, digital commons need to ensure that the risks to those who are included are minimised and effective harm mitigation mechanisms are in place in case harms do occur. To meet the latter goal, it is important that those who contribute to the commons are not excluded from partaking in its governance.

There are four types of exclusion that need to be considered: (a) exclusion from (personal or other) data and information *entering* a digital commons; (b) exclusion of people from *using* data and information held in the digital commons; (c) exclusion of people from *benefitting* from the digital commons (both data and infrastructure); and (d) exclusion of people from participation in the *governance* of the commons (Table 3).

When somebody is prevented from having her personal data (or data and information that she generated) included in a digital commons (scenario A), and when this exclusion is unjust and it negatively affects her fundamental needs and interests (such as her access to healthcare, credit, etc.), then such exclusion should be avoided. A way to avoid it would be to give people in such a situation the legal right to have their data and information included in the commons.[25] An example would be a digital data and information commons for public health surveillance where those whose data and information were excluded could suffer significant harms from policy decisions that do not meet their needs.[26] Such exclusion would be unjust if the reasons for exclusion lie in factors that have no legitimate bearing on the purpose of the database, such as excluding people merely because they do not have Internet access, or who are not included in electoral registers. In such cases, legal provisions should give everybody the right to have their data included (provided that quality and other objective inclusion criteria are met). At the same time, because such inclusion does not only have benefits for the data subject but can also bear risks, it would be important to ensure that governance and harm mitigation mechanisms are in place to reduce risks and mitigate or even compensate for harms.

A similar argument can be made for cases where people are prevented from using, or benefitting from, data and information held in digital commons, or where those contributing to the commons are prevented from participating in its governance (Table 3, Scenario B to D). These forms of exclusion are to be avoided if they are unjust[27] and if they negatively affect the fundamental needs and interest of those who are excluded.

Table 3. Guide to critical reflection on the effects of four types of exclusion from digital commons.

A. *Exclusion from including one's (personal or other) data and information in a digital commons*	
Is the exclusion unjust? *And*: Does this exclusion negatively affect fundamental needs and interests of the excluded?	
(Both questions answered with) *Yes*:	(At least one question answered with) *No*:
1. consider legal obligation to include, and 2. ensure that appropriate governance and harm mitigation mechanisms in place	1. implement mechanisms for voluntary participation, with critical reflection on factual and formal barriers for inclusion, 2. consider how people who are not included in the commons are affected by the commons. Consider possible benefits and harms, and 3. mitigate possible undue harms
B. *Exclusion from using data and information held in the digital commons*	
Is the exclusion unjust? *And*: Does this exclusion negatively affect fundamental needs and interests of the excluded?	
(Both questions answered with) *Yes*:	(At least one question answered with) *No*:
1. consider legal obligation to mandate use rights, 2. ensure that appropriate governance and harm mitigation mechanisms are in place, and 3. ensuring that those who invest in the commons are compensated for use by others who do not invest, if appropriate	1. consider how people who cannot use data and information held in the commons are affected by the commons. Consider possible benefits and harms, and 2. mitigate possible undue harms
C. *Exclusion from benefitting from the digital commons*	
Is the exclusion unjust? *And*: Does this exclusion negatively affect fundamental needs and interests of the excluded?	
(Both questions answered with) *Yes*:	(At least one question answered with) *No*:
1. consider legal obligation to include everybody in the commons, or alternatively 2. consider public provision of the same benefits that the digital commons provides	1. consider how people who do not benefit from the commons are affected by the commons, and 2. mitigate possible undue harms
D. *Exclusion from governance*	
Is the exclusion unjust? *And*: Does this exclusion negatively affect fundamental needs and interests of the excluded?	
(Both questions answered with) *Yes*:	(At least one question answered with) *No*:
1. consider legal obligation to give every contributor the possibility to participate in governance	1. consider how contributors are excluded from governance of the commons affected by the commons, and 2. mitigate possible undue harms

Source: Author.

Also here, we should resort to legal provisions that give people the right to inclusion.

All digital data and information commons that prevent people who seek to participate from contributing to, using, or benefitting from the resource, or who exclude some contributors from the governance of the commons, should have mechanisms in place to scrutinise practices and requirements that have bearing on undue exclusion, as well as the effects that such exclusion would have on the public value of the dataset, and on those whose data and information excluded.[28] Equally, justice considerations should guide the development of every digital commons.

Once questions about undue conclusion have been adequately considered, can other lessons learned from the governance of physical commons be helpful at all for devising rules of governance for digital commons? I have argued that we cannot merely assume that digital commons are common-pool resources and transpose the design principles for physical commons to them to ensure good governance. We can, however, adjust and expand these design principles to better suit digital commons (Table 4). First, although it is impossible to clearly define the boundaries of the digital data and information commons both in terms of the core resource and the membership of the commons, we can develop criteria to determine what is within the scope of the commons and what is beyond. For example, a commons comprising people's health data could include all personal data and information that

Table 4. Adjusted and amended schematic summary of Ostrom's principles for the governance of common-pool resources, adjusted and amended for digital commons.

1	*Clear criteria exist to determine what is within the scope of the commons and what is outside*
2	*Governance rules are well matched to the nature and purpose of the commons*
3	*Governance mechanisms include regular reflection on the categories, practices, and effects of exclusion and inclusion*
4	*The commons does not exclude unduly (i.e., exclusion is not unjust and does not negatively affect fundamental needs and interests of the excluded)*
5	Mechanisms for inclusive collective decision making exist
6	Accountable monitoring of appropriators exists
7	Graduated sanctions in case of rule violations exist
8	Fast and inexpensive conflict resolution exists
9	The self-governance of appropriators of the commons is recognised
10	*Access to effective harm mitigation instruments exists*

Adapted from Ostrom (1990). Italics mark adjustments and amendments.

they consider relevant for their health; or they could include all data that was generated in clinical contexts, regardless of where they are held. We can also try to ensure that the governance rules are well matched to the *nature* of the commons; Ostrom's original requirement of matching governance rules to local conditions features here in the sense that the nature of digital data and information commons is also shaped by the practices and circumstances of the localities where data and information are created and used. To reflect the emphasis on critically scrutinising the categories, processes, and effects of exclusion, governance rules should provide for regular reflection on these, to ensure that the commons do not unduly exclude. Moreover, because risk minimisation in the context of data use is not sufficient to avoid harm, digital data and information commons should also have good harm mitigation instruments. Table 4 contains a schematic summary of Ostrom's principles for the governance of common-pool resources, adjusted and amended for digital commons.

Conclusion

This article started out with a discussion of the idea of Big Data and of the growing power of for-profit corporations in this domain. For some authors, the best way to counteract the overarching power of corporations is to expand the control that people have over their digital data and information at the individual level. Other authors within what I have called the *Collective Control* approach see digital data and information commons as a way in which the collective power of data subjects can be exercised.

I argued that because of the multiplicity of digital data and information, we cannot simply assume that digital commons are (like) physical common-pool resources and apply the design principles developed for these to digital commons. I proposed that explicit attention to the processes, categories and effects of exclusion from digital data and information commons is an important step in designing principles for digital data and information commons. Moreover, structured attention to who, how, and what is excluded from digital data and information commons, to what effects, and how we can prevent undue and harmful exclusion would also enable us to create commons that effectively counteract current asymmetries in terms of resources and power. It will also help to avoid the spread of a commons rhetoric that ultimately seeks to foster the interests of those who are already privileged and powerful in the digital data world. As De Peuter and Dyer-Witheford (2010: 31) have observed, the

> term commons has come to cover a proliferation of proposals, some highly radical, but also some reformist, and others even potentially reactionary. As George Caffentzis points out, neoliberal capital, confronting the debacle of free-market policies, is turning to 'Plan B': limited versions of commons – be it carbon trading models, community development schemes, biotechnology research, and opensource practices – are introduced as subordinate aspects of a capitalist economy. Here voluntary cooperation does not so much subvert capital as subsidize it.

In a world in which digital data and information are such an important political, economic and social

resource, it is important to create digital data and information commons that enhance public value and public benefit[29] – regardless of whether it is a health data commons that includes all people in a country, or an artistic commons that includes only those with an interest in a specific topic or art form. Importantly, some digital data and information collections that are currently not organised as commons might need to be turned into such by law – if we are serious about avoiding significant harm to those excluded.

Acknowledgements

I am grateful to Edward (Ted) Dove, Flavia Fossati, Carrie Friese, Klaus Hoeyer, Hanna Kienzler, Federica Lucivero, Katharina Paul, Nadezhda Purtova, Tamar Sharon, Wanda Spahl, Jeremias Stadlmair, Alice Vadrot, and Hendrik Wagenaar for helpful comments and discussions. The usual disclaimer applies.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. What is often referred to as the 'five Vs' of Big Data also includes veracity. For reasons that will become apparent in the course of the paper I am not including this in my own list.
2. I am grateful to Alberto Giubilini for helpful discussions on this point.
3. This argument is mostly made in connection with provisions for data portability or the right to erasure, see Rubinstein, 2013; Swire and Lagos, 2013; for counter-arguments see Graef et al. 2017; Purtova, 2017a).
4. Some authors in the *Collective Control* group argue that too much reliance on individual-level control is likely to cause more harm than good, such as people 'defensively guard[ing] anonymized information about themselves', having lost sight of the good things that personal data and information can do for people and societies (Yakowitz, 2011: 4; see also Prainsack and Buyx, 2013).
5. As observed by Linnet Taylor, two main understandings of 'the public good' have been prevalent in this debate: The first is the idea that data should be used to help (public and private) corporations to promote the social good in the public sphere. An instantiation of this is Jane Yakowits' definition of the data commons as comprising 'of the disparate and diffuse collections of data broadly available to researchers with only minimal barrier to entry. We are all in the data commons; information from our tax returns, medical records, and standardized misuse by anonymization'. (Yakowitz, 2011: 2–3). The second understanding sees data as a public good due to its potential to promote global health and mitigate crises and disparities within and across societies (Taylor, 2016: 1–2). The latter strand of scholarship focuses less on who should hold and use data, but how and for whom the benefits of Big Data should unfold. Calls for data sharing and data philanthropy fall in this category (for an overview, see Prainsack, 2017b, chapter 5, 'Just profit?'). The first strand of scholarship, in contrast, pays a lot of attention to ownership of data – both in the legal sense of ownership as in property rights to data, and in the moral sense of ownership as control over, and responsibility for, data. Although many authors writing on data commons are also concerned with the benefits of data use, debates in this strand tend to focus on the creation of digital data and information commons, which are the focus of this paper.
6. Birkinbine (2018: 296) goes as far as saying that we need accounts of the commons 'that incorporate a structural critique of capitalism'.
7. In her 2008 paper on a surge of literature dealing with 'new commons' such as knowledge or health commons, Hess (2008: 6) identified six main reasons (she calls them 'entrypoints') for authors to call certain resources commons: 1. The need to protect a shared resource from enclosure, privatisation or commodification; 2. the observation or action of electronic peer-production or mass collaboration; 3. evidence of new types of tragedies of the commons; 4. the desire to build civic education and common-like thinking; 5. the identification of new or evolving types of commons within traditional commons; and 6. a rediscovery of the commons idea.
8. In the case of state-owned casinos, for example, state authorities allow every person above a certain age to access the venue; in the case of national forests, everybody is allowed to access, etc.
9. Note that open access means something different here the current dominant use of the term referring to the absence of cost barriers in accessing a research output. Examples for open access regimes in the way I use it here include the open sea, or areas where jurisdictions deliberately guarantee access for everyone (e.g., beaches or forests). In the information context of open access regimes, some intellectual property rights can still appertain to the object or resource. I am grateful to Edward Dove for helpful discussions on this point.
10. For example, while the land may technically be owned by the state, the state respects traditional land use rights held by local farmers.
11. Ostrom and her collaborators see the existence of certain property rights as necessary for the good governance of commons. These rights include access (right to enter a defined physical area and enjoy non-subtractive benefits),

extraction (right to obtain resource units or products of a resource system), management (right to regulate internal use patterns and transform the resource by making improvements), exclusion (right to determine who will have access rights and withdrawal rights, and how those rights may be transferred), and alienation (right to sell or lease management and exclusion rights) (Schlager and Ostrom, 1992; see also Hess and Ostrom, 2003).

12. This is reflected also in the definition of a commons that Charlotte Hess (2008: 37) proposed in 2008: 'a commons is a resource shared by a group where the resource is vulnerable to enclosure, overuse and social dilemmas. Unlike a public good, it requires management and protection in order to sustain it'. Although we could plausibly challenge Hess' assumption that public goods do not require management and protection, this definition is instructive also with regard the emphasis on the vulnerability of commons to enclosure, which makes this definition more fitting to digital data and information commons than other, earlier definitions of Ostrom and her collaborators (for a more detailed discussion of the notion of enclosure and exclusion, see below).
13. To be exact, for a resource to meet Heller's definition of 'anticommons', the following conditions need to be met: multiple owners hold effective rights to exclude others from the use of a scarce resource (Heller, 1998: 668). Note that it is the fact that multiple owners each hold elements within a bundle of property rights that distinguishes the anticommons from mere private property (where *one* holder of a bundle of rights can exclude others).
14. For them, commons are open access regimes, meaning that nobody has property rights to a resource and it is difficult to effectively exclude potential appropriators.
15. Nadezhda Purtova's conceptualisation of personal data as 'a system resource [...] encompassing ''reincarnations'' of personal data on various stages of the data flow' (Purtova, 2017b: 206) is particularly helpful in this respect.
16. This generic definition was taken from a website containing key terms pertaining to data protection (EU, 2018).
17. The difference of possession and ownership is that the former describes a physical state and the latter a legal entitlement to enforce exclusive control and transferability. If my friend lends me a book then I possess it but do not own it, which means that I can use it but must not destroy or sell it.
18. What is descried here is an ideal type that is not realised in this form in all European countries.
19. It is argued that this is the case also because property rights protect entitlements in a better way than liability rules: For transfers of property rights, the seller (in this case, the data subject) determines the price of the entitlement, whereas in the case of liability, a person destroying the entitlement pays a predetermined sum that cannot be changed by the owner of the entitlement (Calabresi and Melamed, 1972, cited in Purtova, 2009). As Purtova argues:

> [u]nderstanding the US argument for propertization from the angle of Calabresi and Melamed's definition of property makes it clear that within this analytical framework only property regime offers some degree of control and protection to personal data. Any alternative (liability) rule only secures transfer of personal data, albeit against some objectively defined compensation. (Purtova, 2009: 216)

20. In fact the argument that 'true' anonymisation of data – in the sense that data cannot be traced back to the person they come from – is impossible has led some authors to argue that the only effective way to protect personal data is via treating it as personal property (for an overview see Yakowitz, 2011: 3). In another place, colleagues and I have countered this argument by proposing that the answer to the impossibility of anonymisation should be the enhancement of collective public ownership and control over data, and the strengthening of harm mitigation instruments (Prainsack, 2017a, 2017b; Prainsack and Buyx, 2013, 2016, 2017).
21. Those approaches that treat open access regimes as constitutive for data and information commons face the additional problem of not being able to define who can use the resource and who cannot, so that appropriators are not defined clearly either.
22. Save certain inclusion or exclusion criteria that are applicable to all citizens equally, such as medical indications in publicly owned hospitals, age restrictions or dress codes in publicly owned casinos, forbidden behaviours in public forests, etc.
23. For example, the proposal made by a prominent group of British scholars for the implementation of Universal Basic Services in the UK included the provision of free basic phone and Internet access next to social housing, free bus travel, and meals for those in need (e.g., Portes et al., 2017).
24. Harm is significant when it impacts the life of a person in significant and negative ways, and it is undue when there is no legal or important ethical reason to justify the harm.
25. For commons governed by state property regimes, this would be relatively easy to do as state authorities are tasked with determining criteria of exclusion and inclusion anyhow. For commons governed by private property regimes, state authorities could mandate certain minimum inclusion criteria by means of regulatory frameworks within which commons can self-govern.
26. How fundamental needs and interests are defined merits a longer discussion than could be provided in this paper. An acceptable – albeit incomplete – answer would be that the reflection could be guided by the fundamental needs

and interests of citizens that legal frameworks and public institutions in a given country acknowledge as such.

27. Exclusion would not be considered unjust, for example, if it applied only to those who did not contribute to the commons although they easily could have (e.g., a digital commons of medical images for training artificial intelligence that somebody freely chose not to contribute their own medical images to). In the case of exclusion from governing the commons, this is problematic only if it affects those who contributed in the commons in the first place, and if it is unjust and negatively affects fundamental needs and interests.
28. The following list of 15 questions was adapted from Prainsack (2017a) for digital data and information commons specifically:

A. Coordination: Who has influence in:
   1. Agenda setting: What is the purpose of the commons? Who should it benefit, and how?
   2. Determining the terms of the execution of the idea/procedural aspects of the data commons
   3. Deciding on intellectual property questions

B. Participation
   4. Who participates (demographic and social parameters of those who participate)? Why, and how do they participate?
   5. What physical (including technological) and financial resources are required to participate?
   6. How much, and what kind of, training, skill, or expertise is required to participate?
   7. Are there cultural, institutional, or other differences in perception and framing of core issues and stakes?

C. Community
   8. What forms of community pre-exist the establishment of the commons, if any? Which new communities does the commons facilitate or give rise to? What is the constitutive factor for the feeling of belonging on the side of the participants?

D. Evaluation:
   9. Who decides what good outcomes are? How?
   10. What happens to the results of these evaluations?

E. Openness:
   11. What data do participants have access to, and how? What can they do with the data?
   12. Who curates/edits/cleans the data?
   13. Is the contribution of all participants adequately acknowledged?

F. Entrepreneurship:
   14. How are the financial needs of the commons met?
   15. How are for-profit and other interests aligned in this commons (and/or do they conflict, and where?)

29. I will discuss the meaning and operationalisation of public value and public benefit in a separate paper.

References

Agrawal A (2002) Common resources and institutional sustainability. In: Ostrom E, Dietz T, Dolsak N, et al. (eds) *The Drama of the Commons*. Washington, DC: National Academy Press, pp. 41–85.

Andrejevic M (2014) Big data, big questions: The big data divide. *International Journal of Communication* 8: 1673–1689.

Benkler Y (2002) Coase's Penguin, or Linux and the nature of the firm. *Yale Law Review* 112(3): 369–446.

Benkler Y (2004) Commons-based strategies and the problems of patents. *Science* 305(5687): 1110–1111.

Benkler Y and Nissenbaum H (2006) Commons-based peer production and virtue. *Journal of Political Philosophy* 14(4): 394–419.

Birkinbine BJ (2018) Commons praxis: Towards a critical political economy of the digital commons. *tripleC* 16(1): 290–305.

Blackstone W (1979 [1765–1769]) Commentaries on the laws of England 2. Book II, Chapter 1, 'Of Property in General'. Available at: http://avalon.law.yale.edu/subject_menus/blackstone.asp (accessed 12 May 2018).

Bollier D (2014) *Think Like a Commoner: A Short Introduction to the Life of the Commons*. Gabriola Island: New Society Publishers.

Bromley D (1990) The commons, property, and common property regimes. In: *Conference paper: Workshop in Political Theory and Polity analysis*. Indiana University, Bloomington, Indiana. Available at http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/443/The_Commons%2c_Property%2c_and_Common_Property_Regimes.pdf?sequence=1&isAllowed=y (accessed 27 May 2018).

Bunnik EM, Janssens ACJ and Schermer MH (2013) A tiered-layered-staged model for informed consent in personal genome testing. *European Journal of Human Genetics* 21(6): 596–601.

Calabresi G and Melamed AD (1972) Property rules, liability rules, and inalienability: One view of the cathedral. *Harvard Law Review* 85: 1089–1128.

Dean J (1996) *Solidarity of strangers: Feminism after identity politics*. California, US: University of California Press.

De Peuter G and Dyer-Witheford N (2010) Commons and cooperatives. *Affinities: A journal of Radical Theory, Culture, and Action* 4(1): 30–56.

van Dijck J (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance Society* 12(2): 199–208.

European Union (EU) (2018) What is personal data? Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (accessed 9 May 2018).

Evans BJ (2016) Barbarians at the gate: Consumer-driven health data commons and the transformation of citizen science. *American Journal of Law and Medicine* 42(4): 651–685.

Feeny D, Berkes F, McCay BJ, et al. (1990) The tragedy of the commons: Twenty-two years later. *Human Ecology* 18(1): 1–19.

Foer F (2017) *World Without Mind: The Existential Threat of Big Tech*. New York: Penguin.

Gitelman L (ed.) (2013) *Raw Data is an Oxymoron*.

Goldston D (2008) Big data: Data wrangling. *Nature* 455(7209): 15.

Graef I, Husovec M and Purtova N (2017) Data portability and data control: Lessons for an emerging concept in EU Law. Tilburg Law School Legal Studies Research Paper Series 22/2017. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 3071875 (accessed 27 May 2018).

Hafen E, Kossmann D and Brand A (2014) Health data cooperatives – Citizen empowerment. *Methods of Information in Medicine* 53(2): 82–86.

Hardin G (1968) The tragedy of the commons. *Science* 162(3859): 1243–1248.

Heller MA (1998) The tragedy of the anticommons: Property in the transition from Marx to markets. *Harvard Law Review* 111(3): 621–688.

Hess C (2008) Mapping the new commons. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 1356835 (accessed 10 May 2018).

Hess C and Ostrom E (2003) Ideas, artifacts, and facilities: Information as a common-pool resource. *Law and Contemporary Problems* 66(1/2): 111–145.

Kang J (1998) Information privacy in cyberspace transactions. *Stanford Law Review* 50: 1193–1294.

Kaye J, Whitley EA, Lund D, et al. (2015) Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics* 23(2): 141–146.

Leonelli S (2016) *Data-Centric Biology: A Philosophical Study*. Chicago: University of Chicago Press.

Lessig L (2009) The tragedy of the innovation commons: Reconciling private claims with public interest. *Journal of Law, Philosophy and Culture* 4: 35–48.

Lessig L (2001) The future of ideas: The fate of the commons in a connected world. Xxx 19–25, 39–44.

Lezaun J and Mongromery CM (2015) The pharmaceutical commons: Sharing and exclusion in global health drug development. *Science, Technology, & Human Values* 40(1): 3–29.

Linebaugh P (2008) *The Magna Carta Manifesto*. Berkeley: University of California Press.

Litman J (1990) The public domain. *Emory Law Journal* 39: 965–1023.

Litman J (2000) Information privacy/information property. *Stanford Law Review* 52: 1283–1313.

Lohmann R (1992) The commons: A multidisciplinary approach to non-profit organization, voluntary action, and philanthropy. *Nonprofit and Voluntary Sector Quarterly* 21(3): 309–324.

McMahon A, Buyx A and Prainsack B (2019) Big data governance needs more collective agency: The role of harm mitigation in the governance of data-rich projects (under review).

Mittelstadt BD and Floridi L (2016) The ethics of big data: Current and foreseeable issues in biomedical contexts. *Science and Engineering Ethics* 22(2): 303–341.

Morozov E (2011) *The Net Delusion: How Not to Liberate the World*. London: Penguin.

Murphy RS (1996) Property rights in personal information: An economic defence of privacy. *Georgetown Law Journal* 84: 2381–217.

Ostrom E (1990) *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press.

Pasquale F (2017) From territorial to functional sovereignty: The case of Amazon. *Law and Political Economy* (6 December). Available at: https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/ (accessed 12 May 2018).

Perry WL (2013) *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation. Available at: www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf (accessed 12 May 2018).

Portes J, Reed H and Percy A; for the Social Prosperity Network at the Institute for Global Prosperity (2017) Social prosperity for the future: A proposal for Universal Basic Services. University College London. Available at: www.ucl.ac.uk/bartlett/igp/news/2017/oct/igps-social-prosperity-network-publishes-uks-first-report-universal-basic-services (accessed 12 May 2018).

Prainsack B (2017a) *Personalized Medicine: Empowered Patients in the 21st Century?* New York City: New York University Press.

Prainsack B (2017b) Research for personalised medicine: Time for solidarity. *Medicine and Law* 36(1): 87–98.

Prainsack B (2019) Data donation: How to resist the iLeviathan. In: Jenny Krutzinna and Luciano Floridi (eds). *The Ethics of Medical Data Donation*. Dordrecht: Springer. pp. 9–22.

Prainsack B and Buyx A (2013) A solidarity-based approach to the governance of research biobanks. *Medical Law Review* 21(1): 71–91.

Prainsack B and Buyx A (2016) Thinking ethical and regulatory frameworks in medicine from the perspective of solidarity on both sides of the Atlantic. *Theoretical Medicine and Bioethics* 37: 489–501.

Prainsack B and Buyx A (2017) *Solidarity in Biomedicine and Beyond*. Cambridge: Cambridge University Press.

Purtova N (2009) Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review* 25(6): 507–521.

Purtova N (2017a) Do property rights in personal data make sense after the Big Data turn? Individual control and transparency. *Journal of Law and Economic Regulation* 10(2).

Purtova N (2017b) Health data for the common good: defining the boundaries and social dilemmas of data commons. In: Adams S, Purtova N and Leenes R (eds) *Under Observation: The Interplay Between E-Health and Surveillance*. Cham: Springer, pp. 177–210.

Rose CM (1998) Canons of property talk, or, Blackstone's anxiety. *The Yale Law Journal* 108(3): 601–632.

Rose CM (2003) Romans, roads, and romantic creators: Traditions of public property in the information age. *Law & Contemporary Problems* 66: 89–96.

Rubinstein IS (2013) Big Data: The end of privacy or a new beginning?. *International Data Privacy Law* 3(2): 74–87.

Schlager E and Ostrom E (1992) Property-rights regimes and natural resources: A conceptual analysis. *Land Economics* 68(3): 249–262.

Shiffman G and Gupta R (2013) Crowdsourcing cyber security: a property rights view of exclusion and theft on the information commons. *International Journal of the Commons* 7(1): 92–112. DOI: http://doi.org/10.18352/ijc.343.

Swire P and Lagos Y (2013) Why the right to data portability likely reduces consumer welfare: Antritrust and privacy critique. *Maryland Law Review* 72(2): 335–380.

Taylor A (2014) *The People's Platform: Taking Back Power and Culture in the Digital Age*. New York: Picador.

Taylor L (2016) The ethics of big data as a public good: Which public? Whose good? Philosophical transactions. *Series A, Mathematical, Physical, and Engineering Sciences* 374(2083): 20160126.

Yakowitz J (2011) Tragedy of the data commons. *Harvard Journal of Law and Technology* 25: 1–67.

Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an informal civilization. *Journal of Information Technology* 30: 75–89.

Zwick D and Dholakia N (2001) Contrasting European and American approaches to privacy in electronic markets: Property right versus civil right. *Electronic Markets* 11(2): 116–120.