Deconstructing datafication's brave new world

DECONSTRUCTING DATAFICATION'S BRAVE NEW WORLD

Nick Couldry

London School of Economics and Political Science

Jun Yu

London School of Economics and Political Science

Abstract

As World Economic Forum's definition of personal data as 'the new "oil" – a valuable resource of the 21st century' (2011: 5) shows, large-scale data processing is increasingly considered the defining feature of contemporary economy and society. Commercial and governmental discourse on data frequently argues its benefits, and so legitimates its continuous and large-scale extraction and processing as the starting-point for developments in specific industries, and potentially as the *basis* for societies as a whole. Against the background of the GDPR, this article unravels how general discourse on data covers over the social practices enabling collection of data, through the analysis of high-profile business reports and case studies of health and education sectors. We show how conceptualisation of data as having a *natural* basis in the everyday world protects data collection from ethical questioning while endorsing the use and free flow of data *within* corporate control, at the expense of its potentially negative impacts on personal autonomy and human freedom.

Keywords: Big Data, Hyperconnectivity, Data collection, Privacy, Autonomy, Dataveillance, Surveillance, Datafication, Adaptive learning, GDPR

Introduction

It is a commonplace that 'data' represents the future of not just humankind, but of all life and things on earth: this is the discourse of Big Data. From this standpoint, 'datafication' – the process whereby life-processes must be converted into streams of data inputs for computer-based processing – is deemed a natural stage of development, even it has already been deconstructed within a critique of the ideology of 'dataism' (Van Dijck, 2014). But the momentum of datafication still goes on growing through the general Internet of Things and developments in specific sectors (e.g. the Internet of Medical Things: Topol, 2015: 1). Meanwhile, debate is growing about the *uses* of data with ever less attention being given to whether data collection, in particular the collection from persons of data relevant to them as persons and the collection from things of data of potential relevance to persons (we encompass both in the term 'personal data'), itself raises problems. This article starts from the premise that the very collection of personal data continues to raise ethical issues to which we must pay attention (Nissenbaum, 2017).

This divergence between two lines of data critique (use versus collection) matters, because it is unclear at present whether emerging regulation of personal data *uses*, in particular through the EU's General Data Protection Regulation (GDPR), will be sufficient to protect people against the harms caused by continuous data *collection*. The

GDPR is based in fundamental human rights concerns, particularly the right to the 'free development of the personality' (Article 2(1) of the German Constitution). This right protects the value and dignity of the person based on free self-determination, requiring the individual's *capability* to control the data and information produced about her/himself (Rouvroy and Poullet, 2009: 49-51). Certainly, the GDPR represents the most radical challenge so far to datafication and is already being incorporated into business practice in the EU and North America, and its significance has been widely acknowledged by Facebook and many other parties in the worldwide debate following the Cambridge Analytica revelations.[1] But the GDPR's preventive force is limited in cases where datafication serves the 'public interest', where consent has been given to data collection or where data processing is necessary for performing a contract to which a data subject is party (Articles 8, 9, 6(1)(b)). But in increasingly many areas of life (health insurance, employment contracts, education contracts with parents) data collection is incorporated as a basic requirement, leaving *unposed* the question of whether data *should be* collected. Indeed, it is now claimed in some quarters that data collection is so pervasive that it should be exempted from legal regulation, with regulation focussing only on data use (a position Nissenbaum (2017) calls 'Big Data Exceptionalism'). We argue in this article against this position, however, and address the potentially negative implications for individual autonomy of naturalising personal data collection.

Our attempt to *deconstruct* discourse about data practices begins with this recognition that the act of data collection today operates on a much more general level, sometimes in arenas outside the remit of the GDPR. It is thus not enough to rely only on legal interventions such as the GDPR, and vital to challenge the general discourse that makes personal data collection seem natural. In foregrounding discursive deconstruction as a tool, this article recalls Van Dijck and Nieborg's (2009) article nearly a decade ago for this journal on the discourses of 'Web 2.0' whose growing mainstream status, they argued, 'urgently begs for deconstruction' (Van Dijck and Nieborg, 2009: 855). We are not of course the first to offer a wider critique of regimes of automated data extraction (see for example Andrejevic, 2013; Cohen, 2017; Fuchs, 2013; Gandy, 1993; Zuboff, 2015); less usual, however, has been to emphasise the 'denaturalisation' of datafication discourse as a tool to open up debate. As is well-established in many fields, static *and* dynamic aspects of the world become closed off from normative *or* epistemological debate when we treat them as if they were 'natural', part of 'nature'. There are important variants of this principle, whether in anthropology (Douglas, 1986), or STS (Bowker and Star, 1999; Espeland and Sauder, 2007; Porter, 1996), but the core idea remains the same. Also, naturalisation is more than reification (Bewes, 2002; Honneth, 2008). In naturalisation, a process is not (or is not only or necessarily) referred to as, or assumed to be, a 'thing'; it is referred to as, or assumed to be, a part of nature, that is, part of the *totality* of things, objects and processes that constitute 'nature'. Nature in this discursive

sense is not necessarily an aspect of physical (for example, astronomical, biological, or zoological) nature, but rather refers to the totality that is always already 'there' in our lifeworld, providing the basis of all specific normative or epistemological questions. Nature is what can be assumed to be 'given' *so that* arguments about anything in particular can start. As such, nature is *distinctively* immune from critique; only by a process of de-naturalisation that unmasks how particular things or processes were first constructed *as* natural, can they be opened up once more to critique.

How could personal data collection have come to *seem* neutral, even natural and necessary? For this, we need to look critically at European but also North American and business discourse about data. As we will see, such discourse (whether general or specific to sectors such as health and education) barely discusses the fact of data collection at all, making any ethical challenge difficult. By deconstructing dominant discourses about datafication, we seek to hold open a space for future normative debate about one of the most important practical shifts in contemporary everyday life: the routinisation of surveillance and the collection of personal data. In the conclusion, we then turn briefly to the normative implications of *not* naturalising personal data collection and instead treating it as potentially problematic from the start.

We conducted between January 2016 and March 2017 an analysis of general discourses about data *and* specific (health and education) discourses, materials that, together, illustrate a range of perspectives on the collection and processing of data. The first dataset comprised two types of source: 20 authoritative publications and reports from the world's leading economic institutions and consultancy firms, including Deloitte, McKinsey, OECD, PricewaterhouseCoopers, United Nations, World Bank, and World Economic Forum ('WEF' hereafter), alongside (in addition to the GDPR) European and US government reports on data issues (France, Holland, the European Union, plus two US White House reports). The second dataset comprised selections from the public discourse (mission statement, annual reports, marketing language, blog posts) of 19 major corporations and research institutions in the health and education industries, including 23andMe, Fitbit, Google DeepMind Health, IBM Watson Health, PatientsLikeMe, and Wellcome Trust (health), and Blackboard, IBM Watson Education, Impero Education, and Pearson Education (education).[2]

The rationale for this selection was as follows. Global consultancies, IGOs and INGOs, in addition to developing blueprints for global business and persuading stakeholders of the *value* of personal data, also play a role in *rationalising* the often contradictory perspectives about data for the general public, and so play a key role in stabilising practice about data. Government reports (from both Europe and the USA) provide examples of

potentially critical policy discourse on data, reflecting the different traditions of thinking about data in Europe and the USA (for example, as a component of fundamental freedom versus an individual market asset), but also the influence of global business discourse. In the health and education sectors, the majority of digital platforms' approaches are grounded in that market-based understanding of data and privacy. We, however, give special attention to corporations in those sectors, because of their important, if contrasting, *practical* applications of data norms. By teasing out the similarities and differences across the *general and specific* discourses, we hope to offer richer insights into a wider process: the naturalisation of personal data collection.

The naturalisation of data itself

The first, and most fundamental, move in naturalising datafication is to state that today's 'world of near-ubiquitous data collection' (White House, 2014a: 4) is natural. This is achieved through the common metaphor of data as a *raw* material with *value*:

> personal data will be the new "oil" – a valuable resource of the 21st century . . . becoming a new type of raw material that's on par with capital and labour (WEF, 2011: 5, 7).

Through this move, data's basis in a prior process *of data collection* is obscured. Sometimes, however, the ownership of this 'natural' asset is *asserted* to be blurred, and so not referable to personal ownership:

> . . . in contrast to the concept of ownership of physical goods, where the owner typically has exclusive rights and control over the good . . . this is not the case for intangibles such as data . . . The digital divide isn't about who owns data – it's about who can put that data to work (OECD, 2015: 195-197).

At times this makes an interesting counterpoint to a more European-driven thinking that rejects the ownership of data and information for a different reason, in part because recognising such ownership:

> > . . . makes it the responsibility of the individual to manage and protect their data, reinforces individualism and ignores the power relationship between consumers and businesses (CNNum, 2014: 30).

A blurring of data ownership is also achieved metaphorically through the common idea that data are 'merely' the 'data exhaust' exuded by people's lives, and so not *ownable* by anyone, until, that is, they are appropriated by corporations for value (UN, 2012: 9). On

this view, the raw material of data needs a further set of processes to establish its value, merging data into larger pools of data assets.

This aggregative logic is understood as applying to corporations in all sectors, but in the health sector (OECD, 2015: 336) in particular, the possibility of *amassing* data on a large scale generates, potentially, an obligation on individuals to submit to the monitoring that supports this. Very little is said here about the rights (or wrongs) of collecting this data from individuals.

The term '*hyper*connectivity'[3] creates a reified explanation of these processes. The term 'hyper' implies moving inexorably to a higher level of organisation. The further effects of hyperconnectivity become then *already* determined: 'the exponential growth of mobile devices, big data, and social media are all drivers of this process of hyperconnectivity. Consequently, we are beginning to see fundamental transformations in society' (WEF, 2012b: xi). Concerns (such as privacy) are occasionally noted (WEF, 2012b: xi), but not discussed in detail; much more common is to expand on the benefits of 'the connectivity and functionality made possible by converged next-generation networks' (WEF, 2012b: 47).

On this view, large-scale data collection facilitates a data-driven *social* transformation without reference to people at all. What then of the infrastructures built upon processes of datafication?

Naturalising the infrastructure for data use

The key features and infrastructures of data *use* are further naturalised by association with certain large-scale outcomes that seem to offer unquestionable benefits.

The first step to naturalising the various infrastructures for using data is the claim that, like raw materials such as water and oil, data has no value *unless used*: 'data *have no intrinsic value*; their value depends on the context of their use' (OECD, 2015: 197; italics added). Although the very idea of 'raw data' is fundamentally problematic (Gitelman, 2013), the notion that data can be refined (UN, 2012: 13; Weigend, 2017) seems to authorise the notion that there is something prior which is 'raw' (at least unrefined). The features that make even unrefined data very different from a 'raw', let alone 'natural', substance are thereby completely obscured (Alaimo and Kallinikos, 2017).

The unobjectionable notion that data, to be useful, must be put to use, when combined with other principles, can generate the much more contentious claim that only data use,

not data collection, has problematic *consequences*: 'Policy attention should focus more on the actual uses of big data and less on its collection and analysis . . . it is the use of data that is the locus where consequences are produced' (White House, 2014b: xii-xiii). This view suits well the common idea that data, like technology, is in itself neutral (WEF, 2013: 3).

But we would argue the availability of data is not natural (only constructed as such). Nor are data 'technologies' neutral, for they are already deep *applications* of underlying computing technologies whose 'neutrality' (or otherwise) depends precisely on how technologies of data processing are applied to aggregate data according to specific designs (boyd and Crawford, 2013; Gitelman, 2013). Talking primarily about data *use* covers this over.

The next key move towards naturalisation involves thinking about all forms of data collection and usage *together* as something with important scaled-up effects: that is, an 'ecology'. This builds on underlying metaphors which naturalise the status of data as such, but also the idea that using data means connecting it up with other data in ever larger datasets: 'Data . . . is not consumed when used; it can be reused to generate value. Data grows ever more connected and valuable with use' (WEF, 2012a: 7).

The power of this metaphor is enhanced by assuming that the ecological feedback loops are virtuous, not vicious, whether in the area of innovation or politics: 'All factors interact and co-evolve within an ICT ecosystem . . . a virtuous circle starts where improvements in one area affect and drive improvements in other areas' (WEF, 2012b: 6). Other principles are then adduced to reinforce this idea of a virtuous circle that *maximises* the flow of data, for example the supposedly 'open nature' of information systems and the value of free flow in social life:

> data-driven innovation leverages the fundamentally open and interconnected nature of information systems and networks . . . The traditional closed security perimeter approach is thus an obstacle to the development of data-driven innovation (OECD, 2015: 209-210).

It is easy to be swept away by this rhetoric and reach the conclusion that any obstruction to the flow of data in space and time is *ipso facto* bad: 'Because future, yet-to-be-discovered uses of data cannot be fully anticipated, a default policy of deleting data in all contexts can be harmful' (WEF, 2013: 12). The 'price' of using free internet services (data collection) can then be presented as not a cost at all, but as simply a 'fuel' necessary for broader benefits. Ignoring underlying issues with data collection, it is argued that policy should focus on optimising the free flow and use of data in this new ecological

totality: 'shift the collective mind-set about patient data to "share, with protections," rather than "protect" . . . data sharing could be made the default' (McKinsey, 2013: 13). One European government report offers a challenge to this perspective, urging that individuals get back 'full control over the data concerning their online activities and over the implications of the use of this data' (CNNum, 2014: 9), by, for instance, introducing expiry dates for consent given for data retrieval and the use of specific data over time. But this reservation is not reflected in the mainstream of global business discourse which is likely to have much wider influence.

Macro-arguments for datafication

Larger models for thinking about datafication and its long-term benefits move even further from any consideration of data collection.

The most obvious macro-benefit is economic benefit, that is, the production of profits and growth: 'big data can play a significant economic role to the benefit not only of private commerce but also of national economies and their citizens' (McKinsey, 2011: 1-2). A second macro-benefit is improved knowledge and potentially the enhancement of life itself through improved human understanding (WEF, 2011: 5). Here, 'pro-social' arguments, on the benefits of 'sharing . . . communicating and hyperconnectivity' (WEF,

2012b: 118), further naturalise both the general inevitability (as goal) and the necessity (as means) of automated data collection and processing. The claimed outcome is individual *and* social *empowerment*, but there is little reference to the potential negative implications for empowerment of data collection that datafication requires:

> some of the most profound insights are coming from understanding how individuals themselves are creating, sharing and using personal data . . . The impact of this "empowered individual" is just beginning to be felt (WEF, 2011: 7).

> online communities not only provide a place for members to support each other, but also contain knowledge that can be mined for public health research, monitoring, and other health-related activities (OECD, 2015: 351).

These forms of 'empowerment' then allow for a further macro-benefit: a datafied 'common good', to which we return below. A 2014 White House Report is rare in at least seeing some light and shade in the debate, yet it still too slides quickly past data collection and onto issues of use:

> These collections of data are benign, in the sense that they are necessary for products and services that consumers will knowingly demand. Their challenges to privacy arise

> both from the fact that their analog sensors necessarily collect more information than is minimally necessary for their function . . . and also because their data practically cry out for secondary uses ranging from innovative new products to marketing bonanzas to criminal exploits (White House, 2014b: 16).

Occasionally in the literature there surfaces the crucial point that datafication matters not only for social benefits, but also for power and government, that is, by producing 'actionable' intelligence (Amoore, 2013): 'today's analytics must go beyond data input and output and maintain relevance to the real world . . . transforming the data into *actionable information*' (WEF, 2012b: 90; italics added). But this is where the long-term social implications of datafication – as a large-scale process of organising the world through continuous surveillance – come into view.

New data subjects, new privacy

At this point, two deeper forms of naturalising argument are needed: one that rethinks the individual subject in general and the other (next subsection) that rethinks the structure of a datafied social world. Given the potentially negative implications for datafication for the subject's autonomy, it is unsurprising that contemporary discourse on data seeks to reshape our understanding of the subject itself. Reconceptualising the individual as newly

'connected' to multiple information and data gathering systems, involves not just empowerment, but also data-related mutual *responsibilities*:

> Individually, we are all limited in what we can know, but together hyperconnectivity makes it possible to overcome those individual limitations and mine different types of data to find insights (WEF, 2012b: 102).

In so far as these 'shared' rights and responsibilities depend on all parties' use of underlying infrastructures for data collection and sharing, the implications of such infrastructures for personal autonomy are hidden from discussion, since they are what must *already be in place* if the 'new deal' on data is to proceed.

This potential shift in how the human subject is understood is reflected, indirectly, in a US and European discussions of changes in the nature of privacy:

> the physical sanctity of the home's papers and effects is rapidly becoming an empty legal vessel. The home is also the central locus of Brandeis' "right to be left alone." This right is also increasingly fragile . . . [as] people bring sensors into their homes whose immediate purpose is to provide convenience, safety, and security (White House, 2014b: 15).

> Individual privacy rights are only legally triggered by the principle of individual harm, which is not something that often happens in the case of Big Data. The fact that your data are part of a massive data analysis often fails to meet the threshold of individual harm (WRR, 2017: 15).

Meanwhile, a different form of naturalisation (the discourse of the data commons) works to recontextualise datafication within a new vision of democracy, far removed from individuals' potential concerns with the collection of personal data.

Achieving the 'Data Commons'

There are few more resonant terms to capture the collective freedoms associated with the internet than 'the commons' (Lessig, 1999). The notion of the 'data commons' seems to capture a *state* of social well-being achieved through datafication that, according to some writers (Rifkin, 2013), makes historical notions of individual privacy obsolescent. But insofar as discussion of this 'data commons' operates without reference to the possible negative implications of data collection for individual autonomy, its use serves only to naturalise further such processes.

The ‘data commons’ debate has been advanced particularly by the WEF. It is a domain ‘in which . . . information [about health, education, and financial services collected by mobile devices and online platforms] benefits society as a whole’ (WEF, 2012c: 3-4; compare UN, 2012: 17). However, when the costs and benefits of a data commons are set out more fully, the costs of data collection are nowhere mentioned:

> the fear that digital medical data will be *used* by employers or insurance companies to discriminate against individuals is a serious and valid concern. However, this needs to be balanced with the value that the data creates for individuals in terms of better treatment, the value for society in terms of better research and cures, and the value for governments and other healthcare providers in terms of reduced costs (WEF, 2012a: 20; italics added).

Similar ideas, without the use of the term ‘data commons’, are also reflected in such concepts as ‘information commons’ (CNNum, 2014: 31) or ‘data ecosystem’ (UN, 2012: 17). A later WEF report, however, goes further, arguing that restrictions on data use must be limited if the data commons is to grow (WEF, 2013: 8). From this perspective, the basic trade-off of the internet’s development – free services in return for data collection – appears a good deal to gain a larger benefit (the data commons). The OECD makes this trade-off explicit:

> **Promoting open data and data commons**: . . . Advocates for greater openness and transparency link the availability of government data and information to more socially inclusive service delivery; to participatory democracy; and to economic stimulation from the development of new products and services (OECD, 2015: 359; emphasis in original).

Yet none of this acknowledges the possible shifts in the purposes of data use that the data commons involves, let alone the underlying social costs of data collection, and the possible rights of data subjects to object to changes of use. The notion of 'data *commons*' remains in any case metaphorical: it is not proposed that data actually be owned in-common by everyone, only that it be gathered together under wider corporate control.

Some counter-arguments against unfettered data collection

There are rare places in the general reports analysed where the costs of data collection are acknowledged, even if not developed fully:

> Integrating Internet connectivity into devices and things opens up new risks that information will be unintentionally put into the hands of people who should not have

> access to it . . . The outcome for our hyperconnected world might not necessarily be Big Brother, but it might not be far off either (WEF, 2012b: 50, 55).

More broadly, a more critical White House report notes how big data analytics may have 'an immediate effect on a person's surrounding environment or decisions being made about his or her life' (White House, 2014a: 5, linking to resources of the US Constitution (both First and Fourth Amendment)) which points in a very different direction from the 'data commons':

> Flowing from this protection of physical spaces and tangible assets [by The Fourth Amendment] is a broader sense of *respect for security and dignity that is indispensable both to personal well-being and to the functioning of democratic society* . . . "Privacy" . . . addresses a range of concerns reflecting different types of intrusion into a person's sense of self (White House, 2014a: 11; italics added).

A broader critique, however, is made in the European reports. For instance, the French Digital Council calls for a review of the emerging economic and social landscape, rejecting the market-based proposal (Lanier, 2014; Lessig, 1999) of tradable individual property rights in 'own' data:

> Is it [i.e. data] an unsaleable asset, a common asset, private transferable property, or a right of use or usage? There are . . . issues concerning the enforcement of fundamental freedoms (CNNum, 2014: 9, 30).

The French report not only problematises the idea that data is a naturally existing entity, but makes a bridge to thinking about the consequences of data collection from the perspective of 'fundamental freedoms' (CNNum, 2014: 29). A recent Dutch government report similarly claims that automated and ubiquitous collection and extraction of data undermines the 'social space between the individual and others' that helps keep the individual apart from 'institutions that want to observe and direct our behaviour' (WRR, 2017: 7). Big data, it argues, must be used 'in a way that serves to protect *both* personal and social freedom' (WRR, 2017: 7; italics added).

Both the Dutch and French Councils therefore challenge the discourse that data and its collection/use are a natural part of human life in the big data era, in ways that parallel the principles underlying the GDPR. The gulf, however, between these cases of European policy thinking and the general data discourse of world business organisations remains. Let us now explore how that general discourse that naturalises data collection is applied in two contrasting sectors, health and education, where US and UK corporations, operating with a more market-oriented notion of data, are dominant.

Domains of natural datafication: the Health and Education sectors

So far, we have established how a general hegemonic discourse, with few exceptions, covers over the fact of collecting personal data and displaces attention to specific uses, indeed supposed benefits, of personal data. If we are right about the influence of this discourse, we would expect to see similar moves repeated in specific sectors, such as health and education, and this is indeed what we find for North America and the UK. We plan to analyse the distinctive features of these sectors more fully in separate articles, but there are reasons for highlighting these sectors briefly here: education, because it is where we expect mature human subjects to be formed, and so might expect the GDPR's concern with the right of self-development of the personality to be most vigorously protected; and health, because health data is given special treatment in the GDPR as a sector where public interest can be expected to override individual rights (see especially Article 9(2)(h), (i) and (j)). Discussion of the collection of personal data remains, however, limited in crucial ways, as we note below, developing concerns in specialist critical literature.

First of all, both health and education sectors' discourse about big data follows the pattern already seen of shifting the focus from the problems related to data collection towards those associated with data use:

> With new data becoming [naturally] available, innovators have taken the opportunity to build applications that make it easier to share and analyze information. As discussed later in this paper, these advances are starting to improve healthcare quality and reduce costs (McKinsey, 2013: 5).

> The proliferation of technology has created more data and at the same time has made it more accessible; educators just need the tools to put it to work to shape more personalized learning (IBM Watson Education).

Individuals' involvement in the health and education systems is presented here as *naturally* generating vast quantities of meaningful data that can be garnered continuously. Consequently, expanded forms of data collection are ready to be treated as authorised in both health and education cases, legitimating commercial use of the collected data. The argument goes that the automated mining and processing of data (as natural resource) will enhance the service and care offered to individual data subjects. In a recent study, for instance, Lupton (2016a) provided a useful account of how different modes of 'self-tracking' (more or less voluntary) are advocated as a means to achieve better health. Examples from our analysis, in line with those findings, include: data 'support medical professionals as they make decisions' (IBM Watson Health), or help teachers 'respond in

real-time to each individual's performance and activity on the system' (Knewton, Adaptive Learning White Paper). Yet, no limit is discussed on the type and amount of data that can be collected, as long as the data is anonymised, de-identified, or otherwise 'does not reveal your identity' (according to clothing and fitness apparel retailer Under Armour).

These discourses help us imagine a new environment, in which the logic of data-sharing and unrestricted data flow become the *starting-point* for advancing health and education domains and, potentially, society as a whole. Elsewhere, health platforms talk more broadly of 'deliver[ing] a complete, connected, and fun *experience* that's 24/7' (Fitbit; italics added). This deep expansion of data generation and data collection is presented as a *natural* unfolding, fulfilling the dream of hyperconnectivity. Meanwhile, any discussion of the potential costs of datafication, for example privacy and human autonomy, is sidestepped. Let us now see how this general discourse plays out under the specific circumstances of each domain.

The health sector

The use of data in the health and health-related sectors has been relatively well discussed (for example, Lupton, 2016a, 2016b; Neff, 2013; Neff and Nafus, 2016). With the historic

sensitivity regarding health data's confidentiality, health data actors tend to rely on *consensual* data sharing aimed at social benefits on a large scale (but note Lupton, 2016: 7-10 on 'pushed self-tracking' and 'communal self-tracking'). For that reason, alongside data companies' assurances of protecting data through anonymisation and de-identification are claims throughout the health sector that data sharing is a means *to make common life better*. Combining two prominent cases: 'When people share their [health and medical] experiences, they help each other live better' (PatientsLikeMe), and so 'make a real difference to people's lives across the world' (Google DeepMind Health). At the same time, encouragements to share data address individuals in terms of their assumed affinity with other individuals doing, or being, the same: 'A male in his 40's will see that there are 4.5 MILLION other people in the database today – that are JUST LIKE YOU' (IBM Newsroom). Such discourse arguably takes the most radical form when genetic data companies like 23andMe seek to mobilise the general public to rethink their individual rights, by drawing on the human race's *genetic* commonality as the anchor for a new kind of 'community': 'Coming together as a global genetic family can only help all of us understand how we are genetically related to the world around us. (Remember we are 99.9 percent genetically the same!)' (23andMe).

Just as we saw the general discourse of a 'data commons' supplementing the idea of new data subjects, here we find a vision of a newly empowered and connected human

community mobilised to encourage a cumulative practice of data sharing that extends into more general aspects of life and, arguably, produces a more nuanced picture of how health care is enacted and experienced today (Ruckenstein and Schüll, 2017). In such vision, sometimes data and the infrastructures installed to support its collection and use generate new forms of value and reorder relationships between the agents involved in the practices of health care, by blurring the previously existing distinction between different types of medical data and clinical practices (Hogle, 2016). But underneath this discourse are signs of a more fundamental reorganisation of health care itself, with datafication becoming part of a wider neoliberal repositioning of the individual in relation to health care (Clarke et al., 2003): people acquire an *ethical* responsibility to contribute to the common good by caring for themselves, including, quite possibly, by submitting to continuous health tracking. Rights to privacy and freedom, where they restrict information flow to specific contexts, should, some argue, be overridden, since 'privacy has hindered the effective development of new treatments and shared understanding of how to manage disease' (PatientsLikeMe).

This move however, in the context of a health sector which treats patient confidentiality as a basic principle, puts heavy reliance on the idea that personal health data can be securely anonymised. That goes against the grain of recent work in health and genetics law which casts doubt on the sustainability of anonymisation of individual data (Evans,

2016: 5; Kaplan, 2015). To the extent that the anonymisation of health data *cannot* be trusted, we are required to return to this article's more basic question: *should* personal health data be collected and under what conditions should it be made available for wider use?

The education sector

In the education sector, the principle of confidentiality is less heavily ingrained, and the logic of automated data collection can operate with fewer initial constraints. This is not to suggest that the education domain entirely ignores privacy concerns or individual confidentiality (see for instance Pearson, 2014b: 55). But it matters that datafication in the education sector has a background in pedagogic monitoring and individual measurement (compare school league tables that from the start exempted some level of individualised data collection from ethical scrutiny). Few roadblocks exist in education to intensified surveillance through datafication, which 'allow[s] individual students to be monitored and tracked through their production of digital data' (Williamson, 2016: 56). The result, potentially, is to transform the very nature and goal of education, and reconfigure ideas of 'good schooling' (Breiter and Jarke, 2016) and good relationships between teachers and learners (Selwyn, 2014).

In the UK and USA, education actors that implement 'adaptive learning' to optimise learning and learning environments through 'the measurement, collection, analysis and reporting of data about learners and their contexts' (Siemens and Gasevic, 2012: 1) are acquiring a new centrality. Adaptive learning is claimed to be 'absolutely data-driven' (Knewton) and, as such, inevitably relies on the transformation of all elements of the educational process into (ideally continuous) data flows about every student. At the same time, adaptive learning is characterised as a superior alternative to the educational model of the pre-datafication era – now described as an *irresponsible* 'factory-model', in which all children *had to* receive the same content in the same manner (IBM Education), impeding 'a deliberate and continuous approach to the improvement of learning and teaching' (Pearson).

As in the health case, we find a clear application of neoliberal logic: individuals appear to have an ethical responsibility to submit to adaptive learning and so to data collection. The result is a deep normalisation of datafication and an emerging education environment of dataveillance, to which schools, students and parents are expected to commit in the name of a 'better education'. In a recent report, Pearson Education employed the metaphor of 'digital ocean' to capture such environment, which can record every single 'fleeting experience' of individuals (Pearson, 2014a). Not only does this analogy give corporations the right to appropriate data in this 'digital ocean', but it also implies that

they *must* do so: otherwise, it is implied, important educational experiences will be lost forever.

Furthermore, in education discourse, the costs of continuous surveillance are not even acknowledged as a risk in their own right. Unlike in the health case, personalised surveillance is presented as *inherent* to the educational process, indeed necessary for its further *personalisation*! It is not that privacy is exactly forgotten; rather, personalised data collection and storage are not presented as surveillance at all, but the expansion of a new notion of 'digital citizenship':

> Real-time monitoring is not about policing kids. Rather, it's about providing opportunities for mentorship, teaching and learning . . . This allows students to be responsible, safe and good digital citizens – both in school and out in the world (Impero Education, 2016).

The links between continuous surveillance and the education of children are so deeply naturalised here that the panopticon of teachers monitoring pupils in real-time appears neither chilling nor threatening. On the contrary, such possibilities are emphasised as a selling-point, giving teachers 'a full bird's eye view of the entire classroom' (Impero Education), which enables them to 'immediately intervene a highly personalized way'

(Blackboard). Going further, data collection is imagined to 'create a virtuous circle of real-time data that solves issues relating to student leavers lacking necessary skills' (IBM, 2016), and 'allow[s]' children to become good digital citizens.

What is the consequence of this failure even to pose the question of whether personal educational data *should* continuously be collected, stored and used? It is to naturalise something rather shocking: how the free space where students develop and grow as adults and *emerge into* responsible, educated citizens – a space always in modernity assumed to be integral to what education *is* (Dewey, 1938) – has installed within it today an apparatus of continuous surveillance and behaviour modulation (Cohen, 2017). In the brave new world of datafied education, surveillance becomes a paradoxical *condition of* educational freedom:

> the idea [of digital monitoring] is to allow students the online freedom they need to grow, learn and survive in a digital world, with the safety net of keyword monitoring to protect against the risks (Impero Education, 2016).

The main drive behind this combination of adaptive learning and continuous dataveillance is encapsulated in Pearson Education's mission: 'to help people make *measurable progress* in their lives through learning' (Pearson; italics added). The issue

here is not so much measurement itself as the implicit rethinking of the young human subject of education as an entity that needs to be continuously tracked and measured *in order to* become 'free'. This paradoxical notion of freedom, and how freedom can be learned, has major implications for the teacher's role. As Selwyn notes (2014: 52), knowledge about whether a student is 'effective' or 'deviant' may now be obtained primarily through observation of data, relegating teachers to the role of moderators of system evaluations. This changes fundamentally the relationship between teachers and taught, with the former coming to see pupils less through the 'mutual experience of interaction' in the classroom (Dewey, 1938) and more through the metrics of collected data.

Conclusion: Reopening the ethics of datafication

In this article we have shown how deconstructing those discourses, both general and specific, that serve to naturalise not only particular uses of personal data, but the underlying collection of data from persons reconnects contemporary debates about Big Data with the fundamental insight that 'the principal business model of the internet is based in mass surveillance' (Schneier, 2013). This is the truth that Big Data Exceptionalism tries to move past. Continuous surveillance (more precisely, for image- and text-based modalities, 'dataveillance': Clarke, 1988; Van Dijck, 2014) is not *prima*

facie compatible with the practices of democracy, or indeed with principles such as autonomy which are generally assumed to underlie democracy and a good life. This conflict is not therefore something which *can* properly be covered over, without introducing a fundamental contradiction into everyday life.

The European Community's GDPR (in force from late May 2018) acknowledges this fact far more decisively than legal provision in North America, starting out from the recognition that data processing (if not necessarily data collection) affects people's 'fundamental rights and freedoms' (Recitals (1)-(2)), and linking also, if only in passing, to the principle of 'human dignity' (Article 88; see Floridi, 2016). These normative values give the GDPR a different character, as a discourse, from those market-driven business discourses analysed in this article which in most cases start, unproblematically, from the 'facts' of a changed everyday practice. But, as noted earlier, the GDPR will not intervene in arrangements for data collection and processing that have been consented to or contractually agreed, and is framed only in terms of the protection of the *data subject* from arrangements which process *their* data, rather than protecting individuals from the impacts of a *generalised environment* of data collection (Davenport, 2014). There is good reason, therefore, to insist on posing questions about the appropriateness of data collection more generally. If 'privacy' (as traditionally protected, for example, through informed consent) is insufficient to address an environment of continuous,

multidirectional data collection (Barocas and Nissenbaum, 2014), we must dig down to the ethical principles which underpin privacy as a broader norm (Hildebrandt, 2015).

The beginnings of a consensus may be emerging around the value of autonomy, as the basis for challenging assumptions about the naturalness of the continuous collection of personal data. Autonomy can be understood in terms of the individual subject's space of freedom, the 'breathing room' it needs for an ethical life (Cohen, 2012: 149). Or it can be expressed in terms of the fear that continuous data collection may have a chilling effect on citizens' 'independent critical faculty' (Cohen, 2000: 1424), a point also found in German legal thinking (Rouvroy and Poullet, 2009). Alternatively, a fundamental objection to data collection can be expressed in terms of a deepened notion of privacy as 'the right to reasonable control over the construction of one's identity' (Hildebrandt, 2015: 80, drawing on Agre, 2001: 7). The US constitutional lawyer Neil Richards argues that redefining 'privacy' to include 'intellectual privacy' would protect against 'surveillance or interference' when a subject is in the process of 'generating ideas' (Richards, 2015: 5), for example, while reading. 'Privacy', understood merely as the right to block interference within a particular physical space, is clearly insufficient to counter continuous online tracking (White House, 2014b).[4]

Whatever the details of these legal proposals, datafication's nature as a set of social relations involving countless institutions and individuals requires us to formulate any intervention in terms of a *social* value which recognises, as for example did the philosophy of Hegel, the deep social grounding of individual freedom (and autonomy) in mutual recognition. For Hegel, freedom was a freedom 'to be with oneself in the other'.[5] Such freedom is not simply a private good, but a value of social life, necessary for the quality of human beings' life together. How, one might ask, can one be 'with oneself' if one is being continuously surveilled by external forces, whether state or corporation?[6]

If it is at all plausible that the continuous collection of data raises questions for autonomy and freedom in this sense, then it is vital that, rather than naturalising the collection of data as a fact of life, we hold open the question of whether such data collection is ethically appropriate or not. That requires deconstructing, as we have done, those discourses that perform just that naturalisation: general discourses about big data's economic value and applied discourses about the collection and use of data in health and education.

Debates about the normative implications of collecting and processing personal data will no doubt continue, since they underpin new forms of social knowledge, indeed an emerging social order. They are at the heart of the worldwide debate that the Facebook/Cambridge Analytica scandal launched. Deconstruction will never by itself be

enough, but we hope to have shown that, without attention to the task of deconstructing increasingly standardised discourses about data, we lack a basic tool in the much needed debate about datafication's consequences for social freedom.

Funding

The authors gratefully acknowledge the financial support of the Enhancing Life programme (http://enhancinglife.uchicago.edu/), funded by the John Templeton Foundation and administered by the University of Chicago, which funded this research under the project title 'The Price of Connection'.

References

23andMe. Available at: https://www.23andme.com/ (accessed 10 September 2017)

Agre P (2001) Introduction. In: Agre P and Rotenberg M (eds) *Technology and Privacy*. Cambridge, MA: MIT Press, pp.1–28.

Alaimo C and Kallinikos J (2017) Computing the Everyday. *The Information Society* 33(4): 175–191.

Amoore L (2013) *The Politics of Possibility*. Durham: Duke University Press.

Andrejevic M (2013) *Infoglut*. New York: Routledge.

Bewes T (2002) *Reification, or The Anxiety of Late Capitalism*. London: Verso.

Blackboard. Available at: http://www.blackboard.com/ (accessed 12 September 2017)

Barocas S and Nissenbaum H (2014) Big Data's End Run Around Anonymity and Consent. In: Lane J, Stodden V, Bender S and Nissenbaum H (eds) *Privacy Big Data, and the Public Good.* New York: Cambridge University Press, pp.44–75.

boyd d and Crawford K (2012) Critical Questions for Big Data. *Information, Communication and Society* 15(5): 662–679.

Bowker GC and Star SL (1999) *Sorting Things Out*. Cambridge, MA: MIT Press.

Breiter A and Jarke J (2016) Datafying education. *Communicative Figurations Working Papers, No. 11*. Available at:

http://www.kommunikative-figurationen.de/fileadmin/redak_kofi/Arbeitspapiere/CoFi_EWP_No-11_Breiter_Jarke.pdf (accessed 15 September 2017)

Clarke AE, Shim JK, Mamo L, Fosket JR and Fishman JR (2003) Biomedicalization. *American Sociological Review* 68(2): 161–194.

Clarke R (1988) Information Technology and Dataveillance. *Communications of the ACM* 31(5): 498–512.

CNNum [French Digital Council] (2014) Platform Neutrality. Opinion no. 2014-2 of the French Digital Council on platform neutrality, May 2014. Available at: https://ec.europa.eu/futurium/en/system/files/ged/platformneutrality_va.pdf (accessed 10 September 2017)

Cohen J (2000) Examined Lives. *Stanford Law Review* 52(5): 1373–1438.

Cohen J (2012) *Configuring the Networked Self*. New Haven, CT: Yale University Press.

Cohen J (2017) The Biopolitical Public Domain. *Philosophy and Technology*. Available at: https://doi.org/10.1007/s13347-017-0258-2 (accessed 20 September 2017)

Couldry N and Mejias U (forthcoming 2019) *Colonized by Data.* Stanford, CA: Stanford University Press.

Davenport TH (2014) *Big Data at Work*. Boston, MA: Harvard Business School Publishing Corporation.

Dewey J (1938) *Experience and Education*. New York: Collier Books.

Douglas M (1986) *How Institutions Think*. Syracuse, NY: Syracuse University Press.

Espeland WN and Sauder M (2007) Rankings and Reactivity. *American Journal of Sociology* 113(1): 1–40.

European Commission (2015) Fact Sheet: Questions and Answers – Data protection reform. Available at: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (accessed 20 September 2017)

European General Data Protection Regulation (GDPR) (2016) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. Official Journal of the European Union. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 20 September 2017)

Evans B (2016) Barbarians at the Gate. *American Journal of Law and Medicine* 42(4): 651–686.

Fitbit. Available at: https://www.fitbit.com/uk (accessed 10 September 2017)

Floridi L (2016) On Human Dignity as a Foundation for the Right to Privacy. *Philosophy of Technology* 29(4): 307–312.

Fuchs C (2013) Political Economy and Surveillance Theory. *Critical Sociology* 39(5): 671–687.

Gandy OH (1993) *The Panoptic Sort.* Boulder, CO: Westview Press.

(The) German Constitution. Available at:

https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html (accessed 10 September 2017)

Giroux H (1998) Education Incorporated? Corporate Culture and the Challenge of Public Schooling. *Educational Leadership* 56(2): 12–17.

Gitelman L (ed) (2013) *"Raw Data" Is an Oxymoron*. Cambridge, MA: MIT Press.

Google DeepMind Health. Available at: https://deepmind.com/health.html (accessed 10 September 2017)

Hildebrandt M (2015) *Smart Technology and the End(s) of Law.* Cheltenham: Edward Elgar.

Hogle LF (2016) Data-intensive resourcing in healthcare. *BioSocieties* 11(3): 372–393.

Honneth A (2008) *Reification*. Jay M (ed). Oxford: Oxford University Press.

Hornung G and Schnabel C (2009) Data protection in Germany I. *Computer Law and Security Review* 25(1): 84–88.

Ibarra IA, Goff L, Hernandez DJ, Lanier J and Wely G (2017) Should We Treat Data as Labor? Moving Beyond 'Free'. *American Economic Association Papers & Proceedings* 1(1): forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093683 (accessed 3 January 2018)

IBM (2016) First IBM Watson Education App for iPad Delivers Personalized Learning for K-12 Teachers and Students. Available at: http://www-03.ibm.com/press/us/en/pressrelease/50815.wss (accessed 10 September 2017)

IBM Education. Available at: https://www-935.ibm.com/industries/education/learning.html (accessed 20 September 2017)

IBM Newsroom. Available at: https://www-03.ibm.com/press/us/en/index.wss (accessed 20 September 2017)

IBM Watson Education. Available at: https://www.ibm.com/watson/education/ (accessed 20 September 2017)

IBM Watson Health. Available at: https://www.ibm.com/watson/health/ (accessed 20 September 2017)

Impero Education. Available at: https://www.imperosoftware.com/ (accessed 20 September 2017)

Impero Education (2016) digital citizenship: a holistic primer. white paper. Available at: http://www.learningnetwork.ac.nz/shared/professionalReading/DIGCIT.pdf (accessed 20 September 2017)

Kaplan B (2015) Selling Health Data. *Cambridge Quarterly of Healthcare Ethics* 24(3): 256–271.

Knewton. Available at: https://www.knewton.com (accessed 10 October 2017)

Knewton, Adaptive Learning White Paper. Available at: https://www.knewton.com/wp-content/uploads/knewton-adaptive-learning-whitepaper.pdf (accessed 10 October 2017)

Lanier J (2014) *Who Owns the Future?* New York: Simon and Schuster.

Lessig L (1999) Keynote Address: Commons and Code. *Fordham Intellectual Property, Media and Entertainment Law Journal* 9(2): 404–419.

Lupton D (2016a) The diverse domains of quantified selves. *Economy and Society* 45(1): 101–122.

Lupton D (2016b) *The Quantified Self*. Cambridge: Polity.

McKinsey (2011) *Big Data: The next frontier for innovation, competition, and productivity*. Report, McKinsey Global Institute, June.

McKinsey (2013) *The 'big data' revolution in healthcare*. Report, McKinsey and Company, January.

Neff G (2013) Why big data won't cure us. *Big Data* 1(3): 117–123.

Neff G and Nafus D (2016) *Self-Tracking*. Cambridge, MA: MIT Press.

Nissenbaum H (2017) Deregulating Collection: Must Privacy Give Way to Use Regulation? Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3092282 (accessed 10 January 2018)

OECD (2015) *Data-Driven Innovation*. Paris: OECD Publishing.

PatientsLikeMe. Available at: https://www.patientslikeme.com/ (accessed 15 September 2017)

Pearson. Available at: https://www.pearson.com/ (accessed 15 September 2017)

Pearson (2014a) *Impacts of the Digital Ocean on Education*. Report, February 2014. Available at: https://www.pearson.com/content/dam/one-dot-com/one-dot-com/global/Files/about-pearson/innovation/open-ideas/DigitalOcean.pdf (accessed 15 September 2017)

Pearson (2014b) *Preparing for a Renaissance in Assessment.* Report, December 2014. Available at:

https://www.pearson.com/content/dam/one-dot-com/one-dot-com/uk/documents/educator/primary/preparing_for_a_renaissance_in_assessment_and_summary_text_december_2014.pdf

Pippin R (2008) *Hegel's Practical Philosophy.* Cambridge: Cambridge University Press.

Porter TM (1996) *Trust in Numbers*. Princeton, NJ: Princeton University Press.

Quan-Haase A and Wellman B (2005) Hyperconnected Net Work. Working Paper Series, KMDI-WP-2005-2, 9 June 2005. Available at: https://pdfs.semanticscholar.org/41ec/9ad4f369d6ff7610554739b7c9ee0752d7cd.pdf (accessed 05 September 2017)

Richards N (2015) *Intellectual Privacy*. New York: Oxford University Press.

Rifkin J (2013) *The Zero Marginal Cost Society*. New York: Palgrave Macmillan.

Rouvroy A and Poullet Y (2009) The right to informational self-determination and the value of self-development. In: Gutwirth S, Poullet Y, De Hert P, De Terwangne C and Nouwt S (eds) *Reinventing Data Protection?* New York: Springer, pp.45–76.

Ruckenstein M and Schüll ND (2017) The Datafication of Health. *Annual Review of Anthropology* 46: 261–278.

Schneier B (2013) The Public-Private Surveillance Partnership. *Bloomberg View*, 31 July. Available at: https://www.bloomberg.com/view/articles/2013-07-31/the-public-private-surveillance-partnership (accessed 05 September 2017)

Selwyn N (2014) *Digital Technology and the Contemporary University*. Oxon: Routledge.

Siemens G and Gasevic D (2012) Guest Editorial – Learning and Knowledge Analytics. *Educational Technology and Society* 15(3): 1–2.

Topol E (2015) *The Patient Will See You Now.* New York: Basic Books.

Under Armour. Privacy policy. Available at: https://account.underarmour.com/privacy?embedded=1 (accessed 10 September 2017)

United Nations (2012) *Big Data for Development*. Report, United Nations Global Pulse, May.

Van Dijck J (2014) Datafication, dataism and dataveillance. *Surveillance and Society* 12(2): 197–208.

Van Dijck J and Nieborg D (2009) Wikinomics and its discontents. *New Media and Society* 11(5): 855–874.

WRR [The Netherlands Scientific Council for Government Policy] (2017) Big Data and Security Policies. WRR-Policy Brief 6, January 2017. Available at: https://english.wrr.nl/binaries/wrr-eng/documents/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom/WRR_PB6_BigDataAndSecurityPolicies.pdf (accessed 10 September 2017)

Weigend A (2017) *Data for the People*. New York: Basic Books.

White House (2014a) *Big Data: Seizing Opportunities, Preserving Values*. Report for the Executive Office of the President, May. Available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (accessed 10 September 2017)

White House (2014b) *Big Data and Privacy*. Report for the Executive Office of the President, May. Available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (accessed 10 September 2017)

Williamson B (2016) Calculating Children in the Dataveillance School. In: Taylor E and Rooney T (eds) *Surveillance Futures*. London: Routledge, pp.50–66.

(The) Wired (2002) Born Digital. The Wired, 01 September. Available at: https://www.wired.com/2002/09/borndigital/ (accessed 20 September 2017)

Wolf G (2010) The Data-Driven Life. The New York Times, 28 April. Available at: http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?mcubz=1 (accessed 20 September 2017)

World Economic Forum (2011) *Personal Data: The Emergence of a New Asset Class*. Report, January. Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 10 September 2017)

World Economic Forum (2012a) *Rethinking Personal Data*. Report, May. Available at: http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (accessed 10 September 2017)

World Economic Forum (2012b) *The Global Information Technology Report 2012*. Report. Available at: http://www3.weforum.org/docs/Global_IT_Report_2012.pdf (accessed 10 September 2017)

World Economic Forum (2012c) *Big Data, Big Impact*. Report. Available at: http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf (accessed 10 September 2017)

World Economic Forum (2013) *Unlocking the Value of Personal Data*. Report, February. Available at: http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (accessed 10 September 2017)

World Economic Forum (2015) *The Global Information Technology Report 2015*. Report. Available at:

http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf (accessed 10 September 2017)

Zuboff S (2015) Big Other. *Journal of Information Technology* 30(1): 75–89.

[1] See recently the positive acknowledgement of the GDPR in Ibarra et al. (2017), two of whose authors are Microsoft researchers.

[2] Such sources have regularly changing websites and so are cited without date, but with the authors' last access date.

[3] Until the late 1990s, the term 'hyperconnectivity' was mostly used in the contexts of brain research or clinical studies (e.g. to refer to deep connectivity between neural nodes and nerves). Quan-Haase and Wellman (2005) introduce the term in a new media-related sense as: '[t]he availability of people for communication anywhere and anytime' (p.4).

[4] For an alternative formulation in terms of 'human dignity' broadly consistent with the position offered here, see Floridi (2016).

[5] Hegel, *Encyclopedia in Collected Works*, vol. 8, page 84, quoted by Pippin (2008: 186).

[6] For further discussion see Couldry and Mejias (forthcoming 2019: Chapter 4).