Snower, Dennis J.; Twomey, Paul

Working Paper

Humanistic digital governance

Kiel Working Paper, No. 2178

Provided in Cooperation with:
Kiel Institute for the World Economy – Leibniz Center for Research on Global Economic Challenges

Suggested Citation: Snower, Dennis J.; Twomey, Paul (2020) : Humanistic digital governance, Kiel Working Paper, No. 2178, Kiel Institute for the World Economy (IfW), Kiel

This Version is available at:
https://hdl.handle.net/10419/229164

KIEL INSTITUTE FOR THE WORLD ECONOMY

KIEL WORKING PAPER

Humanistic Digital Governance*

No. 2178 December 2020

Dennis J. Snower† and Paul Twomey‡

Kiel Institute for the World Economy
ISSN 1862–1155

Leibniz Association

KIEL INSTITUTE FOR THE WORLD ECONOMY

ABSTRACT

HUMANISTIC DIGITAL GOVERNANCE*

Dennis J. Snower† and Paul Twomey‡

We identify an important feature of current digital governance systems: "third-party funded digital barter": consumers of digital services get many digital services for free (or under- priced) and in return have personal information about themselves collected for free. In addition, the digital consumers receive advertising and other forms of influence from the third parties that fund the digital services. The interests of the third-party funders are not well-aligned with the interests of the digital consumers. This fundamental flaw of current digital governance systems is responsible for an array of serious problems, including inequities, inefficiencies, manipulation of digital consumers, as well as dangers to social cohesion and democracy. We present four policy guidelines that aim to correct this flaw by shifting control of personal data from the data aggregators and their third-party funders to the digital consumers. The proposals cover "official data" that require official authentication, "privy data" that is either generated by the data subjects about themselves or by a second parties, and "collective data." The proposals put each of these data types under the individual or collective control of the data subjects. There are also proposals to mitigate asymmetries of information and market power.

Keywords: Digital governance, digital services, personal data, digital service providers, market power, advertising, preference manipulation

JEL classification: O33, P34, O35, O36, O38, H41, L41, L44, L51

* The authors thank Maria Farrell and Ian Brown for their significant, substantive contributions to this paper. They are also indebted to Jeff Arsenault, Laura DeNardis, Jonathan Fenton, Colm Kelly, John Klensin, Kirsten Martin, Rebecca McKinnon, Mike Orszag, Anouk Ruhaak and Blair Sheppard for extremely insightful comments.

† President, Global Solutions Initiative; Professor, Hertie School of Governance; Fellow, The New Institute, Hamburg; Senior Research Fellow, Blavatnik School of Government, Oxford University; Non-resident Fellow, Brookings Institution.

‡ Fellow and Core Theme Leader, Global Solutions Initiative; Distinguished Fellow, Centre for International Governance Innovation; Commissioner of the Global Commission for Internet Governance; former CEO of ICANN.

Dennis Snower **Paul Twomey**

Humanistic Digital Governance

Introduction

The paper asks a simple question: Who really governs digital personal data? By this question we mean: In whose interests is digital personal data extracted, stored, manipulated and disseminated?

The question is analogous to the one concerning the interests that are meant to guide a competitive market economy. The traditional answer is that "the consumer is king," which means that a competitive market economy is geared to satisfying the objectives of the consumers at minimum resource cost. The reason is that the ultimate purpose of all products is to satisfy the desires of the consumers, either directly (through consumption goods) or indirectly (through investment goods). The consumers pay for the products that they consume and these expenditures drive all other economic activities. More specifically, under ideal conditions,[1] a competitive market economy allocates resources efficiently, so that it is impossible to make anyone better off without making others worse off. Such an economy cannot ensure equity (a fair distribution of resources across the population) and economists usually maintain that this is the responsibility of the government.

So whose interests are primarily satisfied with regard to personal data under the current digital governance regimes? The answer is different from the one above. The reason is that many digital services are provided for free to the consumers – or "users" as they are commonly called in the digital realm. This means that the consumers' expenditures – driven by their underlying desires – are not driving the digital economy. Instead, the digital services are funded by third parties – advertisers, political activists and other influencers – who seek to gain personal data about the consumers and influence their choices. They do so largely outside the consumers' conscious awareness. Even when the consumers consent to the release

[1] These conditions are specified in the First Welfare Theorem of Economics.

of their personal data and to the advertising and other influences they receive, this consent is generally not well informed.[2] The choices that are open to the consumers are generally restricted by the digital service providers; they are not the choices that consumers would be given if the aim was to promote human agency for users in their individual and collective pursuits.

Thus it is not the digital consumers who are in ultimate control of the digital services they receive, the personal data they reveal and the influences to which they are subject. Rather, it is the third-party funders, working with the digital service providers, who ultimately drive the system. Their control is based around large quantities of personal data, much of it collected by data brokers with whom the consumer has no contractual or other relationship, which may be used to manipulate users' preferences to influence purchasing, voting, and many other behaviours (Zuboff, 2019). The third-party interests are ultimately responsible for the digital services that the consumers receive, the personal information that the consumers reveal about themselves, and the ways in which consumers' choices are manipulated. The digital service providers seek personal data about consumers and influence their choices in order to generate advertising revenues or proceeds from the sale of political or social influence. The third-party funders pay for the digital services in order to extract information about the consumers and thereby target their third-party influence more effectively and individually. When the influence takes the form of advertising products, it leads to revenues from these products. When the influence is political and social, it leads to outcomes that state or non-state agents find worth pursuing.

In short, the users are being used by the third-party funders. The interests of the third-party funders are not well aligned with the interests of the users. In this sense, the current

[2] Indeed, as researches at the Brown Institute of Columbia University have shown under their terms and conditions and privacy policies alone, Amazon, Apple, Facebook, and Google collect over 450 different items of information about their users. See https://brown.columbia.edu/mapping-data-flows/

digital governance system is not humanistic. It does not place ultimate value on the agency of the human beings using the digital services. It is not designed to promote the fundamental needs and purposes of these humans, as individuals and as social creatures. It is not inherently concerned with the promotion of human freedom, empowerment and social belonging.

The digital revolution has unleashed a tidal wave of new opportunities for gaining information quickly and cheaply, improving the efficiency of our design, production and marketing systems, gaining access to goods and services (such as through online shopping and online booking for cabs and hotels), promoting interpersonal exchanges (such as through video calls and webinars), providing new opportunities for pursuing environmental sustainability (such as through more efficient resource and energy use), and much more.

Nevertheless, the misalignment of interests between the third-party funders and the users is responsible for a wide variety of malfunctions that undercut some of the benefits from the digital revolution of the past 40 years. As explained briefly below, these malfunctions ultimately threaten the continued functioning of our economic market systems; weaken mental health, expose users to far-ranging manipulation of attention, thought, feeling and behavior; erode appreciation for objective notions of truth, undermine our democratic processes; and degrade the cohesion of our societies.

The benefits from the digital revolution are not immutably tied to the current digital governance regimes. There exists no law of nature whereby the benefits from the new digital technologies can only be reaped through third-party finance of digital services to the users, combined with information-gathering and influence-projecting that lies largely beyond the consumers' informed consent. On the contrary, the benefits of the digital revolution are as little tied to the current digital governance regimes as the benefits of the industrial revolution were tied to the exploitative practices of many early factory owners.

The aim of this paper is to consider the technological benefits from the digital revolution as separate from, though influenced by, the current digital governance regimes.

Furthermore, we inquire how these regimes could be made humanistic without sacrificing the technological benefits. In particular, we provide policy guidelines that would put the digital users – the consumers of digital services – into the driver's seat, giving them ultimate control, individually and collectively, over their personal data and the economic, social and political influence to which they are subject.

Humanism in Digital Governance

Humanistic digital governance includes, but goes well beyond, digital consumer protection. While consumer protection aims to safeguard the buyers of goods and services, as well as the general public, from unfair commercial practices, humanistic digital governance aims to ensure that the digital system serves human needs and purposes – namely, those of the consumers of digital services and the general public. A central message of this paper is that (1) humanistic governance (as well as consumer protection) is not realizable in the absence of consumer control over personal data, individually and collectively; and (2) such consumer control over personal data is not realizable in the absence of appropriately defined digital property rights. Under the current digital governance regimes, consumers lack control over the use of their personal data and they do not have individual or collective property rights on data about themselves. Under these circumstances, the quest for consumer protection is doomed to failure.

The appropriately defined property rights go beyond the standard conception of intellectual property rights (IPRs). IPRs are the rights given to individuals over the creations of their own minds for a specified period of time, giving these individuals control over their creations through patents, copyrights, trademarks and trade secrets. The appropriately defined digital property rights, by contrast, are (i) rights of individuals and collectives (not just individuals) (ii) over data about individuals (not merely data that individuals create by and

about themselves), and (iii) the collective rights emerge from the consent by the individuals comprising the collective.

Putting humanism at the center of digital governance involves taking seriously the fundamental human needs and purposes of human beings. It means constructing a digital governance system that recognizes the dignity of the person and serves to promote human flourishing in all its aspects: life and health, empowerment and liberty, love and social embeddedness, and sustainable relations with nature. It means deploying information and the resulting knowledge in the name of such human flourishing, both individually and collectively. It involves recognizing that humans are both individuals who require freedom and social creatures who derive life meaning in conducting personal relationships and belonging to social groups, both of their own choosing. It also involves the acknowledgement that much of life fulfilment emerges from participation in the service of others – other humans and other sentient beings.

Consequently a humanistic digital governance system is designed to promote not only the consumption of goods and services (which are the focus of economic analysis), but also the need for agency and solidarity within planetary boundaries. These needs are present in all cultures. They are not fully substitutable for one another. For example, it is not possible to compensate a person for the cost of solitary confinement by providing more consumption. Since these needs are fundamental, the benefits from pursuing and satisfying them cannot all be measured in monetary terms (such as dollars or euros). The SAGE dashboard by Miranda and Snower (2020) captures such fundamental needs in terms of Solidarity, Agency, material Gain, and Environmental sustainability. The satisfaction of these fundamental needs is also implicit in the UN Sustainable Development Goals and the OECD Better Life Index, as well as other measures of wellbeing.

While competitive free market activity can (under ideal conditions) lead to economic efficiency, in accordance with the mechanism that Adam Smith identified as the Invisible

Hand, there is no mechanism whereby such market activity automatically leads to social solidarity, personal empowerment or environmental sustainability. In all these areas, some combination of government policies, economic institutions, social norms and moral values are called for.

The problems associated with the current digital governance regimes – inefficiencies, inequities, asymmetries of market power and information, manipulation of consumer preferences, inadequate protection of privacy, etc. – may all be understood as violations of fundamental human needs and purposes. For example, the inequities and asymmetries of power and information are violations of social solidarity, while consumer manipulation and infringements of privacy are violations of agency.

Currently these problems in the digital domain are addressed largely in isolation from one another, for example, through competition law, privacy law, intellectual property legislation, consumer protection legislation, commercial law, and more. We argue, however, that since these problems may all be understood as symptoms of a common cause – the systemic dysfunctions of the current digital governance regimes – the existing policies could be powerfully supplemented through humanistic digital governance.

To this end, we propose four broad policy guidelines, each of which serve the purpose of moving control over personal data from the third-party funders and digital service providers to the users of digital services. The thrust of this movement is to be understood as analogous to the gradual readjustment of power in much of the offline world, from overbearing monarchs and monopolists to a broader set of stakeholders, including consumers and employees. The underlying principles of social justice are the same online as offline. There is much that we can learn in the online world from the ways in which these principles were pursued in the offline world.

One important historical experience in this regard is that the gradual shift of economic power from monarchs and feudal lords to small-scale entrepreneurs, who made their living by

responding to their consumers' demands, is acknowledged as an important driver of early capitalism. Furthermore, the shift of power from domineering industrialists toward a more balanced relationship between employers, employees and customers from the middle of the 19th century to the middle of the 20th century in the advanced industrialized countries was an important factor in the spread of the "mixed economy" (containing free enterprise, supplemented by government finance and provision of education, health, social security and other areas) after World War II. These experiences suggest that the appeal of humanism – in particular, its emphasis on individual and collective empowerment – has played a significant role in the spread of humanistic economic relations. This leads us to believe that humanistic digital governance may prove to be successful in the digital realm for the same reasons.

In broad outline, the world may currently be divided into five governance regimes: (i) the American regime, in which a small number of digital service providers enjoy preponderant market power and digital information advantages, (ii) the Chinese regime, in which the state enjoys preponderant informational advantages, supported by a small number of digital service providers, (iii) the European regime, in which digital service providers are far less powerful and the state's regulatory power focuses on protecting the rights of digital users, (iv) other middle economies, many of whom are democracies, which similarly are concerned about the power of the big American and Chinese platforms but lack the negotiating power of the EU, and (v) the rest of the digital world, primarily comprising emerging economies, with little market power and little regulatory power, but a strong drive to narrow the digital divide. Due to the inherent popularity of governance regimes that promote individual and collective empowerment, the option of humanistic digital governance is relevant for all of these regimes. But there is no reason to believe that humanistic digital governance is likely to be adopted in the same form across all four regimes, much as the mixed economy as not been adopted in the same form across countries. In the offline world, Anglo-Saxon free market economies coexist with European social market economies, state-

guided capitalist economies, and more.[3] These economic systems are thoroughly integrated in global value chains, trading goods and services and moving financial and physical capital. Along analogous lines, different digital governance regimes may be expected to connect with one another through the exchange of information in accordance with mutually agreed terms. Humanistic digital principles may be relevant to these regimes in the same way as the principles of voluntary exchange have been relevant to the diverse mixed economies. In the offline world, feudalism, slavery, indentured servitude, child labor and other institutionally exploitative practices have gradually been replaced by more humanistic ones, despite the institutional and cultural diversity. The same may be expected in the digital realm, but in fast motion.

At present, the EU digital governance regime is most closely aligned with the humanistic principles advocated here. In fact, our proposed policy guidelines are already compatible with the EU's General Data Protection Regulation (GDPR), the Digital Services Act package[4] and other EU digital directives and acts. As such, they can be understood as a simplification and development of existing legislation. Such has been the lure of humanistic governance systems in the past, that we have reason to expect a similar attraction to digital governance regimes in the future. We claim that the more the EU digital governance regimes adheres to the policy guidelines articulated here, the more economic activity – both digital services and the associated non-digital goods and services – will be attracted to the EU area. On this account, humanistic digital governance may become an important influence on digital regimes elsewhere as well.

---

3 There are many other typologies. For example, Esping-Andersen's (1990) influential typology of welfare capitalism covers "Liberal regimes," with limited means-tested assistance, "Conservative regimes," with family-based assistance and "Social democratic regimes," with universalistic systems focused on equality rather than minimal needs.

4 https://ec.europa.eu/digital-single-market/en/digital-services-act-package

Dysfunctions of the Current Digital Governance Regimes: Servitude 2.0

To understand the fundamental problem of the current digital governance regimes, consider a new form of servitude, call it "Servitude 2.0." Slaves provide free labour for their owners; in return, the owners give them free food, clothing and shelter. This may be considered a form of barter: free labor for free provisions. Furthermore – this is the new feature of Servitude 2.0 – slaves are free to leave their owners whenever they wish, but when they do so, they must leave everything behind – their belongings, their friends and acquaintances, their reputation and all other external aspects of their identity. Is this system likely to be efficient and equitable?

The obvious answer is "Of course not!" There is no assurance that the value of the slave labor corresponds to the value of the provisions that the slaves receive. There is no market mechanism that sets the marginal value of the slaves' labor equal to the marginal value of the slaves' consumption of provisions. On this account, Servitude 2.0 is likely to be profoundly inefficient. No matter how large the inefficiency, there is no market mechanism to correct it, since the exchange of labor for provisions occurs at zero prices. Furthermore, the slaves have no incentive to acquire the efficient amount of skills, since skill acquisition is not rewarded.

Servitude 2.0 is also likely to be profoundly inequitable. Slave owners – being fewer in number and having more information, expertise and legal backing – have more market power than the slaves. The slave owners are likely to use this market power to extract as much labor for as few provisions as possible. This exercise of market power is likely to make the slave owners rich, while the slaves remain poor. Since the slave owners have more information about the production process involving slave labor than the slaves do, the slaves are not in a position to know what the appropriate remuneration for their labor would be. There is no market mechanism to correct these asymmetries of market power and information, due in part to the exchange at zero prices.

The protection of human rights is not realizable as long as slaves have no control over the amount of work that they provide and over the provisions they receive in return. This control is not realizable in the absence of property rights over the fruits of their labor. Once slaves are freed and able to enter the labor markets, they gain property rights over the remuneration for their labor. They then become able to sell their labor services and buy provisions at terms that they choose, in interaction with the demanders of their labor and the suppliers of their provisions. Under these circumstances, the protection of human rights can be realistically pursued. For example, the state may offer protection to vulnerable workers, provide information about job opportunities (thereby reducing the asymmetry of information), and give workers rights of association (thereby reducing the asymmetry of market power).

This hypothetical system of servitude is relevant for us nowadays, because under the current digital governance regimes, we – the consumers of digital services – tend to be Slaves 2.0. We provide information about ourselves for free. In return, we receive free apps and other internet services. We are free to leave any networks to which we belong, but when we do so, we must leave everything behind – the information about us, our contacts, our ratings, and our digital identities on those networks. We have no property rights on the data we generate, and only by generating such data can we derive benefit from our data aggregators and digital network providers. This free labour enables a complex ecosystem of data aggregators and markets, which are invisible to the vast majority of the people whose personal data are being collected, at the top of which sits a few digital service providers – such as the 'Big Nine' (Apple, Facebook, Amazon, Google, IBM, and Microsoft, Tencent, Baidu and Alibaba) – which have amassed vast fortunes unprecedented in the history of humankind.

This system suffers from a number of serious problems. First, the system is inefficient, since economic markets cannot generate efficiency when the commodities transacted – information about individuals in return for internet services – are free (or under-priced). There is of course

no guarantee that, for every individual, the marginal value of the free internet services is equal to the marginal value of the free information about the users. On the contrary, we have every reason to believe that the value of the information supplied by users to the digital service providers far exceeds the value of the internet services that the users get for free, for otherwise it would be hard to explain why – under allegedly competitive conditions – the digital service providers are able to amass such wealth. People with high skills in generating valuable data have no incentive to employ their talents for this purpose if data are supplied for free. Costless data also gives people no incentive to develop skills that could improve internet services.

These inefficiencies are tolerated by the data aggregators and digital network providers, since what they lose from these inefficiencies they make up handsomely through the market power gained through digital servitude 2.0. Hal Varian, the chief economist at Google, argues that data nowadays are plentiful and thus virtually worthless, whereas the designers of the networks are scarce and thus generate most of the value of the digital network services.[5] This argument is self-serving. It is analogous to arguing that slave labour, in the heydays of slavery, was plentiful and that most of the value was generated by the designers of the slave plantations. It is impossible to assess the marginal contributions of data users and network designers when one of these groups works for free. Furthermore, as Posner and Weyl (2018) note, it is far from clear that the marginal value of the data generated by network users declines with the amount of data, given that the data are used to handle more and more complex problems (such as face and emotion recognition and predictable cognitive processes).

One could argue analogously that just as the value of one consumer's personal data is negligibly small in comparison to the value of the aggregated digital services, so the value of

5 For example, https://mbs.edu/news/hal-varian-from-google-like-oil-data-must-be-refi

one employee's work is negligible in a global supply chain. By this line of reasoning, most of the value comes from combining the work of countless employees working in a variety of countries to produce the commodities generated by the global supply chain. But this is not considered an argument for the reintroduction of slavery, namely, the free exchange of labor services for provisions. This reasoning does not stop the employers from paying all their employees their wages.

Second, the system is inequitable since the owners of the data aggregators and digital network providers wield overwhelming power. They own the access to the digital data on which their users rely, much as old-style slave-owners owned the access to their slaves' basic necessities. The fact that the slave-owners provided something of value to their slaves did not make the exchange of slave labour for basic necessities equitable. The slave-owners were in a position to exploit their market power to their own material advantage, much like the data aggregators and digital network providers nowadays are doing.

The current regime creates major accretions of market power in the hands of the digital service providers, as they are natural monopolies generated by network effects, reinforced by significant user costs of switching among providers as well as informational asymmetries between the data subjects and the digital service providers. The market power asymmetries arise in significant part from the digital services' control of the personal data of their users, who have inadequate options to codetermine the conditions of their network participation.

Since the scale and complexity of data aggregation, the informational asymmetries and many of the switching costs that underlie the concentration of market power are not transparently observable to the data subjects, the market power asymmetries are also opaque. This opacity makes it difficult to correct the market power asymmetries through competition law, which has been designed for dealing with concentrations of power in the traditional markets for goods and services. Further obstacles to the effective regulation of digital

monopolies are their global reach (and the continually emerging opportunities for cross-country profit shifting), their richly endowed lobbying activities, and the abovementioned failure of courts to award damages for probabilistic and uncertain harms.

Third, the system is manipulative, exploiting the psychological weaknesses of the consumers. Digital service providers seek to maximize their users' attention in order to extract maximal revenue from advertising and from the information about users' behaviour that is useful for advertising. On this account, digital services frequently exploit users' vulnerability to negativity bias and loss aversion (in both social and economic terms, paying greater heed to potential losses than to potential gains). Consequently users devote substantially more attention to threats than to positive content and become disproportionately concerned with the bad rather than the good.[6] This undermines their psychic health and promotes social discord.

In addition, digital services frequently exploit users' confirmation bias (the tendency to seek and recall information that confirms one's prior beliefs and to interpret evidence in accord with these beliefs). Thus, in order to attract users' attention, digital service providers tend to expose their users to content that is aligned with their preconceived views. This practice contributes to the social and political fragmentation in many countries, promoting social discord and political conflict.

Fourth, the system is disempowering. Although users are not fully aware of the pervasive means by which their attention is captured through their mobile devices and their preferences are shaped by the content of the information that has been prepared for them, there is nevertheless a widespread sense of powerlessness in the face of overwhelming odds. In order to be properly functional in most advanced and emerging nations, people need to be digitally connected and these connections come prearranged and prefabricated by digital service providers driven by third-party funding.

---

6 See, for example, Baumeister et al. (2001).

Thereby the current regime violates one of the most fundamental human liberties: the liberty to shape one's own social networks in accordance with one's own needs and purposes. This opportunity is substantially highjacked through the power of digital service providers to connect people in accordance with their own rules and instruments of persuasion, grafted into the media whereby people communicate with one another and receive information about their environment. Instead of giving users the freedom to structure their social networks naturally in accordance with their most significant social affiliations in the physical world – affiliations driven by deep personal relationships with people we respect, trust and care for, our social networks are shaped significantly by the objectives of the digital service providers to capture the attention of their users as long as possible, to attract more users, and generate advertising revenue.

The resulting sense of disempowerment is compounded massively by the Internet of Things (IOT), whereby material objects communicate with one another, largely outside the awareness of people. These cyber-physical communications have turned the Internet into a control system in the hands of those who manage the cyber-physical information flow.[7] In practice, people's ownership of objects is thereby undermined, since the material objects are exchanging information and making decisions on this basis without the users' involvement and often in pursuit of the digital service providers' objectives.

Fifth, the system provides inadequate protection of privacy, by design. The GDPR (Article 25) requires data controllers to design and use technologies to enforce data protection rights, by default. But in practice, many of the digital tools (such as smartphones) and services (such as social media) in common use could be characterised as surveillance systems, used particularly by digital service providers to target advertising individually to users. These users consent to this surveillance by agreeing to the terms and conditions of the digital services –

7 For an excellent account of these problems, see DeNardis (2020).

terms and conditions they usually do not attempt to read, and would be unable to read (with all hyperlinks to other relevant documents) even if they wished to, due to the time and effort that would require.[8] In some cases, users have the possibility of opting out of some surveillance, but often in return for significant loss of service.[9]

Finally, the system is frequently destructive of productivity and health. Since digital service providers seek to maximize their users' attention to their services, these services are designed to interrupt our daily tasks with new information and activities, targeted at the users' individual interests. Users are also encouraged to search for information related to targeted stimuli appearing on their screens. These practices degrade our capacities for sustained attention to complex tasks and our patience for pursuing projects at require sustained effort. Users are encouraged to multitask, but the human brain does not multitask in the sense that we understand multitasking in our daily lives; instead it switches rapidly between different activities. This stressful alternation is supported by adrenaline and cortisol, which over the long run makes it difficult for us to be tranquil and content; and it also has an inflammatory influence on our brain cells, which may be linked to depression.[10]

In short, the continuous stimuli we receive through our smartphones and other digital devices hurt our concentration and makes us anxious. Our instinctive response to these stimuli is to remain in a constant state of alertness and assuaging our digital addiction by continuous monitoring of the procession of stimuli while never giving full attention to anything. This

---

8 See, for example, Kaldestad (2016): "The average consumer could easily find themselves having to read more than 250,000 words of app terms and conditions. For most people this is an impossible task, and consumers are effectively giving mobile apps free rein to do almost whatever they want."

9 Apple is one of the few major counter-examples to this trend, although even in this case concerns exist around Apple's plans to profile and advertise to its users, and that privacy is becoming a luxury good rather than fundamental right.

10 Bullmore (2018) examines the link between inflammation and depression.

state of protracted distraction and interruption hurts our cognitive faculties, hurts our intelligence (Gazzaley and Rosen, 2016), and harms our productivity.[11]

We argue that all these problems are symptoms of a fundamental systemic dysfunction, which we call third-party-funded digital barter.

Third-Party-Funded Digital Barter

The current digital governance regimes are supported by the myth that "the internet is free" – a space where everyone, everywhere can share information and collaborate costlessly. Though there are some important success stories in this respect, such as Wikipedia and Sci-Hub, the internet reality usually looks quite different. Many internet services may be costless to the consumers in direct monetary terms, but can be very costly in other terms.

The reason is that the providers of these services usually get two valuable things in return: (i) incredible amounts of personal data about us as consumers, enabling them to target advertising and political influence individually and (ii) the power to influence us as consumers, by capturing our attention and shaping our preferences. These information-gathering and influence-bearing features of internet services generate revenue for the sellers of offline goods and services and the sellers of paid online services. Furthermore, the social and political influence exercised on the digital users aims to encourage social movements and political support that serve the interests of influencers. It is these advertisers and other influencers who pay for the services that the digital consumers get costlessly.

In short, costless internet services are traded for personal information plus the acceptance of a highly sophisticated, intransparent, all-encompassing digital experience through which to be influenced in one's preferences, motives, beliefs, focus of attention and

11 See, for example, Puranik et al. (2019) examines the effects on productivity.

social networks. This is the nature of the exchange that commonly takes place in the digital realm, which we call third-party-funded digital barter.

The digital barter provides no assurance that the value of the personal information about consumers corresponds to the value of the digital services that they receive. This is the source of the inefficiencies noted above. It is also a source of the comparatively low productivity growth that many countries have experienced over the past decade: When digital services are provided at zero price, their contribution cannot enter into the measurements of economic growth (i.e. the proportional growth of GDP). Further, while the influence may be delivered to a consumer in one market, the payment for the advertising often takes place in a handful of other markets – resulting in an erosion of goods-and-services-tax-type revenue in the first country.

Since the digital service providers are natural monopolies that own the personal data in their networks, funded by the influencers who use these networks, and since the consumers – who do not control the data about themselves – have comparatively little market power, the third-party-funded digital barter undermines competition in economic markets.

This asymmetry of market power, accompanied by an analogous asymmetry of information concerning how personal data is collected and used, generates inequalities in the distribution of income and wealth.

The system has a natural tendency to manipulate consumers and exploit their vulnerabilities, since the interests of the third-party funders of the digital barter are not aligned with the interests of the consumers and since the funders and consumers operate in a system characterized by great asymmetries of market power and information.

The asymmetry of information and power associated with third-party-funded digital barter also leads to a natural tendency towards inadequate protection of consumers' privacy.

These asymmetries also lead the digital service providers to give consumers limited choices, such as the choice between remaining connected to their economic and social world

and giving up control over their personal information. These limited choices are responsible for the widespread sense of disempowerment, arising from attention capture, manipulation of preferences, and misleading information.

The drive to capture attention and manipulate consumers' decisions, along with spread of disinformation and hate speech, have adverse effects on consumers' health and productivity.

In these ways, the variety of problems associated with the current digital governance regimes are all symptoms of a fundamental flaw inherent in the third-party-funded digital barter system: the lack of alignment between the interest of the consumers and the interests of the third-party funders working together with the digital service providers.

When policy makers attempt to tackle each of the symptoms in isolation – through competition law, privacy regulations, injunctions against hate speech, directives on consumer rights, laws concerning commercial practices, digital transactions taxes, fines for digital fraud, and much more – these policy makers find themselves engaged in a never-ending battle against systematically inappropriate incentives. The policy measures then become endless catch-up efforts to tackle ever new symptoms of the system's fundamental flaw.

To return to the metaphor of digital servitude 2.0, these policy measures can be compared to attempts to tackle the problems of slavery by addressing its dysfunctional symptoms. For example, breaking up the digital monopolies through competition law is analogous to legislating that slave owners may not own more than a specified number of slaves. Privacy regulations are analogous to decreeing that slave owners are not permitted to enter their slaves' lodgings without the latter's permission. Laws concerning commercial practices are analogous to laws governing the treatment of slaves. Policies to promote digital literacy are analogous to training subsidies for slaves. Consumer protection legislation is analogous to laws specifying minimal standards for treating slaves.

The upshot of these analogies is simple: Digital policies are doomed to remain inadequate as long as the consumers of digital services have artificially restricted choices, such as the choice between revealing large amounts of personal data (by agreeing to the terms and conditions of digital services) and being excluded from most economic and social interactions in this increasingly digitalized world. To ensure that consumers do not face artificially restricted choices, it is necessary to give them control over the data about themselves, individually and collectively.

Since the fundamental flaw of the current digital governance regime is the lack of alignment between the interests of the consumers and the interests of the third-party funders and the digital service providers, policies that address the symptoms of this underlying flaw are likely to be ineffective in combatting the inherent injustices and inefficiencies of the current system. For example, protecting privacy by requiring users to agree to the terms and conditions of digital services cannot ensure informed consent, because these terms and conditions are generally too cumbersome and intransparent for most consumers to read and understand, particularly in the context of complex nested agreements among digital service providers, internet service providers and third-party funders. Furthermore, even if consumers were able to digest all the terms and conditions of their digital services, there would be no assurance that consumers were allowed to choose from a portfolio of options allowing them to satisfy their needs most efficiently.

On this basis, we now proceed our policy guidelines for humanistic digital governance.

Policy Guidelines

We begin with a new classification system for personal data, which permits our proposed policy guidelines to be readily understood.

We distinguish between three types of personal data:

O-Data is "official data" that requires authentication by third parties for the purpose of conducting legally binding transactions and fulfilling other legal obligations. Authentication can come from the state or other legally accepted sources. Examples include one's name, date of birth, professional qualifications, and land registry deeds.

P-Data is "privy data" related to individuals, but which is not collective and does not require authentication by third parties. This data may be divided into "first-party data" (such as personal blogs and personal photographs) that are volunteered or generated by the data subject and observable by other parties, and "second-party data" generated by a second party about the data subject (such as location data from smartphones, records of a person's past purchases of goods and services) or inferred about the data subject from existing data (such as psychological data deduced from web searches).

C-Data is "collective data," which data subjects agree to share within a well-defined group or community of interest for well-defined collective purposes. This data may be shared through voluntary agreements or through democratic processes established through law.[12] C-data is subject to the same security requirements and restrictions on unpermitted onward transit as P-data currently is under data protection laws. This data can encompass consumer associations, agricultural collectives, trade unions, financial collectives and much more.

On this basis, we propose the following four policy guidelines.[13]

12 This definition of "data commons" is not related to common pool resources, since the former is excludable while the latter is not.

13 The practical implementation of these proposals is to be contained in a further paper.

Proposals 1: Control over O-Data

Proposal 1a: O-Data must receive official (Generally Trusted Source) authentication and this is to be the only legal source of this data.
Proposal 1b: Give individuals genuine control over use of their O-Data through easy-to-use technical tools and supporting institutions.

In other words, O-Data is to be controlled by the data subject, but authenticated by trusted third parties, under a new legal framework which makes this record the only way in which such data may be drawn by third parties. This provision gives the data subject the power to allow the collection of the data by a third party and under terms to which the data subject has agreed.[14]

Currently there are few if any laws requiring that all parties must access official data in a uniform way from an authenticated user-controlled source. The appropriate off-line analogy is the European ID card, for which agents (such as hotels) are legally required to collect the data authenticated on the card only from this authoritative source. The key is that legally this is the single source to be used by nominated third parties. The online version requires that a set of data that is authenticated by the state or a generally trusted source be held in an authoritative source under the control of the individual – and that this be the single source for drawing such data fields.[15] Whenever a company or other party requires this data, it

14 It is this power of the data subject that makes meaningful the rights of association to negotiate use of the data with the data aggregators.

15 Our proposal does provide not incentives for data aggregators to replace our O-data with a proprietal unique identifier linked to an avatar of users that the aggregators have built from Second party P-data, permitting the unique identifier to get activated by the aggregator's algorithms when a particular device is detected or allowing the aggregator to infer several data points and then deliver the manipulating data or advertisements without actually needing to know who the users are. This possibility needs to be closed through legislation, analogous to laws against tax evasion.

should not be inferred or observed, but be drawn from the user-controlled authoritative source.[16]

Why does the single source matter? Because it provides the system with a unique legal representation of the individual (not the vast number of versions of the individual which exist with rough functional equivalence in the present ecosystem, many of which the individual does not know exist). And uniqueness means that not only is control of access more easily achieved, but it also bolsters the leverage of the individual – or her agent – to negotiate with companies the financial and use terms for access to this data. It is the fulcrum on which the power between the data aggregator and the individual can be adjusted. [17]

Proposals 2: Control over P-Data

Proposal 2a: The data subject is to be the only legal source of first-party P-Data.

This proposal is analogous to Proposal 1a

16 This requirement is similar to the authoritative root system for a limited set of data which dives the Domain Name System. This is an adaptable technological model for which the technical architecture can be developed straightforwardly. Just as the authoritative data fields in a DNS record are prescribed (open to ongoing standards review and change), so authoritative data fields can be prescribed for first-party private data. More complex technical architectures are also possible, providing stronger privacy protection, such as those designed by the EU-funded DECODE and SPECIAL Horizon 2020 research projects.

17 In the offline world, comprehensive union coverage in industrial and other workplaces empowered large scale collective bargaining – and resulted in a middle class emerging from an industrial working class. The requirement for data aggregators to deal with collective bargaining to get O data of the individual may give similar degrees of leverage for the individual in dealing with global platforms and others.

Proposal 2b: Give individuals genuine control over use of their first-party P-Data, through the above-mentioned technical tools and supporting institutions.

Providing direct, effective control of first-party P-Data calls for mainstream use of new technological and institutional mechanisms for managing personal data, whereby the control of this data is handed from the digital service providers to the data subjects. The implementation of users' right to directly manage and control of their first-party P-Data will build on the system established above for O-Data. First-party P-Data (photos, geo-location data, biometric information, etc.) is placed online by the user in the context of a contractual or other legal relationship with a company (a cloud operator, telco, app provider, employer, etc.) This legal relationship will require the company also to hold the individual's O-Data as part of their account management processes. The individual or her collective bargaining agent, will negotiate financial and use terms for first-party P-Data as part of the right for accessing the authorative O-Data record. These terms will apply to the contract or other legal instrument which links the individual and the company. We expect these terms to also be reinforced by new law requiring that P-Data be held and used in the interests of the data subject.

Proposal 2c: Use second-party P-Data exclusively in the interests of the data subjects.

The governance of consequential second-party P-Data is to be analogous to that in the offline world concerning intimate data that is not held by the data subject, when this data is generated by a second party on behalf of the data subject, such as in doctor-patient or lawyer-client relations. In these cases, the holder of the data is permitted to use the data (and more broadly, act) only in the interests of the data subject (with specific public interest exceptions – for example, reporting suspicions of abuse, or notifiable diseases).[18]

18 When this data is generated by a second party on behalf of a wider group, such as pictures of politicians by journalists or pictures of travelers at border controls, this data may belong to the data commons, as specified by existing laws.

Data that is inferred about the data subject is also to be used only in the interests of the data subject. For this purpose, the data subject needs to have automatic access to the data inferred about him- or herself and to determine what data is to be held by the second party. The inferred data must be transparent and clear, i.e. understood by the data subject in a limited time frame. The terms and conditions that a second party sets for digital services tied to inferred data must be proportionate to the agreed purpose of the data collection. Any actor who collects personal data about an individual should be required to act on, share, or sell this data only if it is consistent with that individual's interests. Data brokers who hold intimate knowledge of individuals need to be held to a fiduciary-like standard of care for how their data may be used (Balkin, 2016). This would make data brokers responsible for how their products and services were used to possibly undermine individual interests.

Putting a legal requirement for companies to use data in the interests of the data subject also demands an objective test to ensure that the interpretation of the "interests of the data subject" is not open to differing interpretations. Various entities and companies could claim to be acting in the individual's interest, as they define it, even if the individual believes they are not. With reference to Europe, we propose that the test be grounded in two existing bodies of law: the European convention on human rights and European law governing relationships between professionals and their data subjects (doctor-patient, lawyer-client etc.), particularly the law related to use of patient/client data so as not to manipulate or exploit the data subject.[19]

The same principle holds for data that is generated by material objects owned by the data subject. The IOT digital service provider, when different from the owner of the material objects, are to manage the IOT data flow in the interests of the data subject and the data

19 Some examination of this law can be found at https://ec.europa.eu/health/sites/health/files/cross_border_care/docs/2018_mapping_patientsrights_frep_en.pdf

subject needs to be given automatic access to the data generated by the relevant material objects. This data, along with associated terms and conditions, must be transparent and clear.

The second party should have a fiduciary duty to ensure that second-party data is used in the interests of the data subject by third parties. Legal protections can be drawn from "fiduciary law" frameworks, which consider the expertise, benefit and confidences in trusted, but informationally imbalanced professional relationships (Balkin, 2016).

Proposals 3: Control over C-Data

Proposal 3a: Create legal structures to support the establishment of 'data commons' for C-Data.

A data commons is a legal entity that protects and uses the data of members to serve defined collective objectives, subject to a fiduciary duty to serve their interests.[20] Like a commons in the offline world – for example, an agricultural or fishing commons – the data commons has clear boundaries, roles, obligations and responsibilities that are developed and used to ensure the medium and long-term collective interests of the community that depends on these resources. In this proposal, a legislative framework is needed to enable and incentivise existing communities of interest to create data commons to collect and use their C-data, including by licensing it to others.

---

20 A data commons is very similar to what in common law countries is known as a 'data trust'. Although the legal concept of a 'trust' does not exist in all countries, many civil law jurisdictions have relevant traditions of agricultural cooperatives, cooperative banks, and related institutional forms. The data commons relies on a broad concept of fiduciary obligations to a defined group of people as a means to ensure the future honouring of legal commitments to safeguard and steward data according to the interests of the data subjects. For a discussion of the difference between a data commons and data trust, see Ruhaak (2020). For the purposes of this paper, the term data commons is used to emphasise both the more widely applicable legal concepts and to invoke the principles of commons management developed by Ostrom (1990) (2010a) (2010b).

The data commons is a defined and protected structure to which people can delegate the stewardship of certain subsets of their P- and O-Data. It may allow other organisations – for example, public bodies, companies, researchers – access to the data, subject to the preferences of the data-subjects and in line with policies set collectively and always in their interests. The members collectively set the terms for how their data is shared and direct where the benefits created should go. Execution of these objectives is delegated to the data commons trustees who must ensure the commons carries out its fiduciary obligations to the data subjects. Also key to ensuring both the conduct of the commons and the overall competitiveness of the data environment is that people's data is portable and practically interoperable. People can withdraw their data and decide not to share it, find an alternative or even create a new data commons to further their collective interests and goals.

This proposal tackles the current lack of incentives and protective structures to support and incentivise groups – e.g. trade unions, agricultural and banking collectives, consumer associations, under-served populations, and even, for example, consumers such as electricity customers – to collect and use their data to further their collective interests. There is currently a gap in the ability of social and economic communities of interest to use their collective data for the group's and society's benefit. This results in the under-provision of certain kinds of societally beneficial data-uses, and a disproportionate concentration of resources on the exploitation of data for advertising.

Proposal 3b: Ensure that C-Data are under the control of effective, trustworthy and competitive organisations that promote the benefits of data subjects and the broader society.

The current system may limit the willingness of citizens to share all forms of their own data, particularly health data, to secure collective goals, because of the potential individual cost and risk to them in an untrustworthy data environment. In some cases, C-Data collected by third parties may even be used to secure anti-competitive advantage against the data subjects, as for

example with regard to farm and cooperative-level agricultural productivity data.[21] Large-scale data-sets about the public – such as smart city data – should be evaluated to assess whether both their value and the risk of misuse merit these data-sets being managed in data trusts or commons, despite a clear fiduciary obligation to the data subjects.

Legislative support is required to create minimum legal definitions, protections and obligations for a range of data commons to be created. Drawing on existing types of organisations including clubs, cooperatives, trade unions and trade associations, legal guidance or definitions will encourage the emergence of data commons that identify and meet currently unmet demand for data-sharing that protects and extends the interests of data-subjects. Legislation may also be needed to ensure data commons identify and carry out the data-sharing policies of subjects and ensure appropriate privacy and security standards are met. The underlying guidelines for management of data-trusts as a commons can be derived from Elinor Ostrom's Core Design Principles on the management of common pool resources.[22]

Proposal 3c: Ensure that the data commons are permitted to use data only for specified purposes and that its use, like that of P-Data, be transparent and accountable.

The relevant application of existing data protection law to C-data covers the existing notice and consent regime for data transfers, as well as requirements for ensuring the security of that data.

Transparency and accountability in the use of second-party P-data and C-data online should be analogous to that used offline. Manipulation works because the tactic is hidden from the target. The governance goal is to make the basis of manipulation visible to the target

21 https://www.platform-investico.nl/artikel/de-datagrarier/ "THE DATA GRANT Data-driven agriculture can lead to animal suffering and farmers' financial misery"

22 See, for example, Ostrom (1990, 2010a,b) and Wilson, Ostrom and Cox (2013).

and others, i.e., make the type of intimate knowledge used in targeting obvious and public. This might mean a notice (e.g., "this ad was placed because the ad network believes you are diabetic") or a registry, during hypertargeting, to allow others to analyse how and why individuals are being targeted.[23] It should not be sufficient for an AI/data aggregator to simply say, "I am collecting all this information in the users' interests to see tailored advertising." That is equivalent to a doctor saying, "I collect all this data about a patient's health to ensure that patients only know about the prescriptions I give them."

Patients have to give permission for data to be collected and are entitled to know what data is involved (indeed, in many countries, patients formally own their health data), what tests have been conducted and their results, what the diagnosis is. They are entitled to a second opinion on the data. In other areas, where a lawyer, realtor or financial advisor has intimate knowledge and could profit in a way that is detrimental to their clients, they must disclose their conflict and the basis for their conflict. Transparency and accountability online and offline could be brought into consonance with each other.

Proposals 4: Addressing Digital Power Asymmetries

The general rule is to address digital power asymmetries along the same lines as in the offline world.

Proposal 4a: Provide effective rights of association for digital users.

Key to addressing power asymmetries is government support for the rights of association of data-subjects.

23 Registering would be particularly important for political advertising so that researchers and regulators can identify the basis for hypertargeting.

The process of negotiating the terms of authorization – who has the right to access an individual's O and P Data records and on what conditions – is the crux of re-empowering the citizens. This ensures that they are aware of who is collecting data on them and to set directly, or through an agent or collective bargaining, the terms on which they allow such data to be collected and used – including the right to refuse such collection. This is a principle which builds on the existing GDPR rights for an individual to be informed about the collection and use of the individual's personal data.

The citizen, either directly or (more likely) through an agent, could set the terms under which he or she receives and approves/denies requests from companies/entities to access and use the citizen's official data records. Such an agent principle reflects the rights of association and of collective bargaining. It also rewards scale or specialization in negotiating the best/most tailored terms with various types of data collectors. Some of these terms will be financial, many may not be.

Data commons are a means for communities of interest to responsively manage their data – including smart city residents, trade union and trade association members, agriculture and aquaculture cooperatives, cooperative banks – in ways that extend association to people and organisations not currently directly involved. To address power asymmetries, data interoperability (Brown, 2020) will be required.

In the labour market, the right of association has enabled trade unions to support workers' rights, and employers' associations to support employers' rights. An analogously effective right of association should be provided to digital users with regard to their personal data. This could build on the notion of collective redress in the GDPR (Article 80).

Proposal 4b: Provide effective legal protection for vulnerable digital users.

In the product market, consumers' rights are supported through consumer protection legislation. Protection against discrimination based on protected characteristics (such as

gender, disability and age) is supported through equality and human rights agencies (e.g. the EU Fundamental Rights Agency). Digital users who are vulnerable to economic, political or social manipulation should receive analogous protection.

Manipulation is only possible because a market actor, in this case a data broker, has intimate knowledge of what makes a target's decision making vulnerable. The combination of intimate knowledge with hypertargeting of individuals should be more closely regulated than blanket targeting based on age and gender. To protect individuals from manipulation in the name of "legitimate interests," individual autonomy, defined as the ability of individuals to be the authentic authors of their own decisions, should be explicitly recognized as a legal right.

As stated above, there is a profound, yet relatively easy to implement, step to address this manipulation. Government can extend the existing regulatory requirements to act in the best interests of the data subject that apply to religious leaders, doctors, teachers, lawyers, government agencies, and others who collect and act on individuals' intimate data to also apply to data aggregators. Without any market pressures, data brokers who hold intimate knowledge of individuals need to be held to a fiduciary-like standard of care for how their data may be used, not least because inferences data traffickers make based on a mosaic of individual information can constitute intimate knowledge about who is vulnerable and when they are vulnerable.[24]

Proposal 4c: Ensure that competition in the online world is analogous to that in the offline world.

Barriers to entry exist in many digital markets due to network effects (the value of services rise with the number of users) and a range of other factors. The treatment of the resulting

24 Under the GDPR, inferences made about individuals are recognised as sensitive information. It provides for rights of access, notification, and correction not only for the data being collected, but also the possible inferences about individuals drawn from the data. Whether these rights, as currently interpreted, are currently effective in protecting individuals may be questioned.

power asymmetries should be treated more analogously to the regulation of natural monopolies offline.[25] Many jurisdictions, including the EU (via the Digital Services Act), have begun the process of legislative reform to re-establish the conditions for effective competition in these markets.

Proposal 4d: Provide GAAP-like oversight to data traffickers with regard to the protecting the data they hold.

Governments can establish a governance structure along the lines of GAAP (Generally Accepted Accounting Principles) to regulate data traffickers and ad networks to ensure individualized data are not used to manipulate. Recently McGeveran (2019) called for a GAAP-like approach to data security, where all firms would be held to a standard similar to the use of GAAP standards in accounting. However, the same concept should also be applied to those who hold user data in terms of how they protect the data when profiting from it.[26] Audits could be used to ensure data traffickers, who control and profit from intimate knowledge of individuals, are abiding by the standards. This would add a cost to those who traffic in customer vulnerabilities and provide a third party to verify that those holding intimate user data act in a way that is in the individuals' interests and prevent firms from capitalizing on their vulnerabilities. A GAAP-like governance structure could be flexible enough to cope with market needs while remaining responsive and protecting individual rights and concerns.

25 For a summary of the literature on the regulation of natural monopolies, see Joskow (2007). For a recent analysis, see Ducci (2020).

26 It is ironic that currently data traffickers can sell data to bad actors but they just can't have their data stolen by those same bad actors.

Concluding Remarks

The policy proposals above are no panacea. In order to ensure that our digital system functions in the best interests of society, it is naturally vital that these proposals be supplemented by a variety of other policy initiatives, such as ones that promote the widespread acquisition of digital skills and steer technological developments in humane directions.

Nevertheless, the proposals above would constitute an important step towards humanistic digital governance since they address the fundamental flaw of the current digital governance regimes, namely, the misalignment of interests between the consumers of digital services (on the one hand) and the third-party funders and digital service providers (on the other). The proposals do so by taking straightforward steps whereby control of personal data is transferred from the digital service providers to the digital users. Under a digital governance system driven by the needs and purposes of the digital users, many of the inefficiencies, inequities, manipulations of consumer preferences, health costs of digital influencing, sources of social conflict and misinformation, and asymmetries of information and market power would be automatically mitigated. Needless to say, the users of digital services have no interest in prolonging these problems. All they need is control over their personal data and support in addressing information and power asymmetries.

References

DeNardis, Laura. (2020). *The Internet in Everything*. Yale University Press.

Esping-Andersen, Gøsta. (1990). *The Three Worlds of Welfare Capitalism*. Princeton University Press.

Balkin, Jack M. (2016). Information Fiduciaries and the First Amendment. *U.C. Davis Law Review* 49 1183.

Baumeister, Roy F., Ellen Bratslavsky, Catrin Finkenauer, and Kathleen D. Vohs. (2001). Bad is Stronger than Good. *Review of General Psychology*. Volume: 5 issue: 4, page(s): 323-370, https://journals.sagepub.com/doi/abs/10.1037/1089-2680.5.4.323.

Brown, I. (2020). Interoperability as a tool for competition regulation. *OpenForum Academy* https://doi.org/10.31228/osf.io/fbvxd

Bullmore, Edward. (2018). *The Inflamed Mind*. Picador.

Ducci, Francesco. (2020), *Natural Monopolies in Digital Platform Markets*. Cambridge University Press.

Gazzaley, Adam, and Larry Rosen. (2016). *The Distracted Mind: Ancient Brains in a High-Tech World*. MIT Press.

Joskow, Paul L. (2007). "Regulation of Natural Monopolies," in A. Mitchell Polinsky & Steven Shavell (eds), *Handbook of Law and Economics*, vol. 2, pp 1227-1348, Elservier. https://economics.mit.edu/files/1180

Kaldestad, Oyvind (2016). „250,000 words of app terms and conditions", Forbruckerradet, May 24, https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/

Lima de Miranda, Katharina, and Dennis J. Snower. (2020). Recoupling Economic and Social Prosperity. *Global Perspectives*, 1(1), 1-30.

McGeveran, William. 2019. The Duty of Data Security. *Minnesota Law Review*. 103: 1135.

Ostrom, E. (1990). *Governing the Commons*. Cambridge University Press.

Ostrom, E. (2010a). Beyond Markets and States: Polycentric Governance of Complex Economic Systems. *American Economic Review*, 100, 1–33.

Ostrom, E. (2010b). Polycentric systems for coping with collective action and global environmental change. *Global Environmental Change*, 20, 550–557.

Posner, E. A. and G. Weyl. (2018). *Radical Markets: Uprooting Captalism and Democracy for a Just Society*. Princeton University Press.

Puranik, Harshad, Joel Koopman, and Heather C. Vough. (2019). Pardon the Interruption: An Integrative Review and Future Research Agenda for Research on Work Interruptions. *Journal of Management*, Nov. 21, https://doi.org/10.1177/0149206319887428

Ruhaak, Anouk. (2020). "Data Trusts: What are They and How Do They Work?" The Royal Society of Arts, https://www.thersa.org/blog/2020/06/data-trusts-protection

Ruhaak, Anouk. (2020). "Data Commons and Data Trusts: What They Are and How They Relate", https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2

Wilson, D.S., E. Ostrom, and M.E. Cox. (2013). Generalizing the Core Design Principles for the Efficacy of Groups. *Journal of Economic Behavior and Organization*, vol. 90, supplement, June, S21-S32. https://doi.org/10.1016/j.jebo.2012.12.010

Zuboff, Shoshanna (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books