Social Macroeconomics

Working Paper Series

Revisiting digital governance

SM-WP-2020-003

September 2020

Dennis Snower, Hertie School of Governance; Blavatnik School of Government, Oxford University; Brookings Institution; and Global Solutions Initiative

Paul Twomey, Biosecurity Systems; Global Solutions Initiative; Center for International Governance Innovation; Global Commission for Internet Governance.

Maria Farrell

Revisiting Digital Governance [1]

by Dennis J. Snower[2], Paul Twomey[3] and Maria Farrell[4]

26 October 2020

Abstract

This paper summarizes an array of problems associated with the current digital governance, which ultimately threaten the continued functioning of our economic market systems, undermine our democratic processes, and degrade the cohesion of our societies. The central claim of the paper is that the benefits of the current system can be retained, while the problems can be overcome substantially through three insights. The first is a new classification system, which permits new policy approaches to be imagined. The second insight comprises three policy proposals, aimed at rectifying the deficiencies of the current governance regime, promoting economic, social and political freedoms and preventing the accretion of large power asymmetries. The third insight concerns implementation options that enable data subjects to gain appropriate control over their personal data.

---

[1] The authors wish to thank Prof. Dr. Ian Brown for his significant, substantive contribution to this paper. They are also indebted to Prof. Dr. Laura DeNardis, Dr. Jonathan Fenton, Colm Kelly, Dr. John Klensin, Rebecca McKinnon, Anouk Ruhaak and Blair Sheppard for extremely insightful comments.
[2] Hertie School of Governance; Blavatnik School of Government, Oxford University; Brookings Institution; and Global Solutions Initiative.
[3] CEO of Biosecurity Systems, Fellow at the Global Solutions Initiative, Distinguished Fellow, at the Center for International Governance Innovation and a Commissioner of the Global Commission for Internet Governance.
[4] Independent writer, speaker and consultant on technology and the future.

1. The Big Idea

The digital revolution of the past 40 years has unleashed a tidal wave of new opportunities for gaining information quickly and cheaply, improving the efficiency of our design, production and marketing systems, and for promoting environmental sustainability. However the current digital governance regimes are beset by serious problems, which ultimately threaten the continued functioning of our economic market systems; weaken mental health, expose users to far-ranging manipulation of attention, thought, feeling and behaviour; undermine our democratic processes; and degrade the cohesion of our societies.

A principal source of these problems is a systemic dysfunction that may be called (with some narrative license) "*third-party-financed digital barter*." Many digital services are provided for free, or under-priced, in return for information about and influence on the digital users. This information and influence is sold to influencersadvertisers and other influencers, such as political and social activists. Thereby the influencersinfluencers shape the users' economic, social and political behaviors in accordance with the influence-selling objectives.

These interactions stand in sharp contrast to the transactions in standard economic markets, where producers sell products to consumers and receive revenue in return, as shown in Figure 1. This trade is "visible," in the sense that it counted in the national income and product accounts.

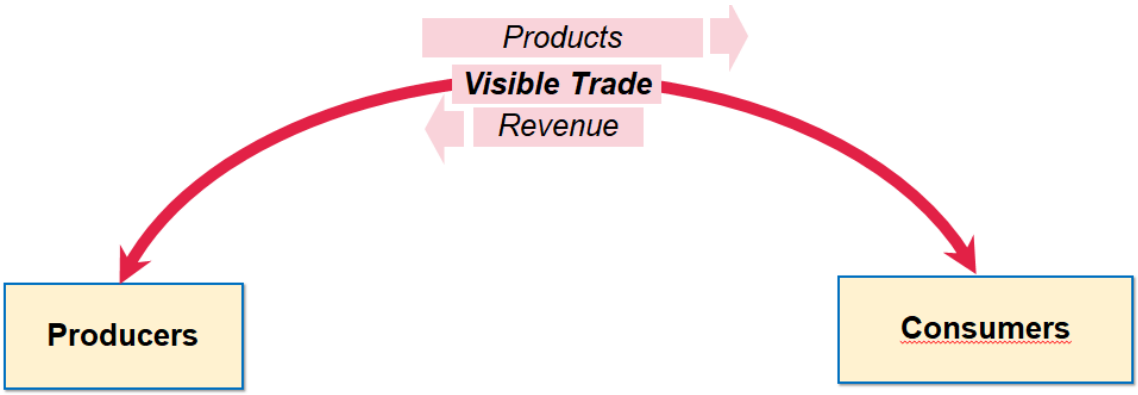

Figure 1: Standard Economic Markets

Under digital barter, however, digital service providers give consumers digital services for free (or under-priced) and, at the same time, gain personal information about the consumers and exert behavioural influence on the consumers. In other words, *the digital barter is both information-gathering and influence-bearing.*

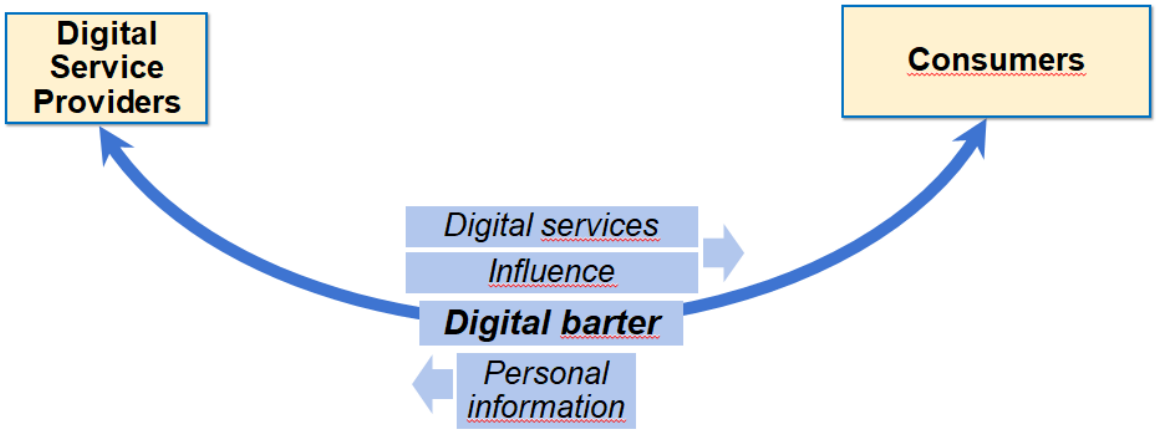

Figure 2: Digital Barter

This digital barter is financed by the influencers (comprising both traditional producers and other influence-wielding parties), who are both the source of the influence flowing from the digital service providers to the consumers and the destination of the personal information flowing from the consumers to the digital service providers. The resulting economic system is pictured in Figure 3.

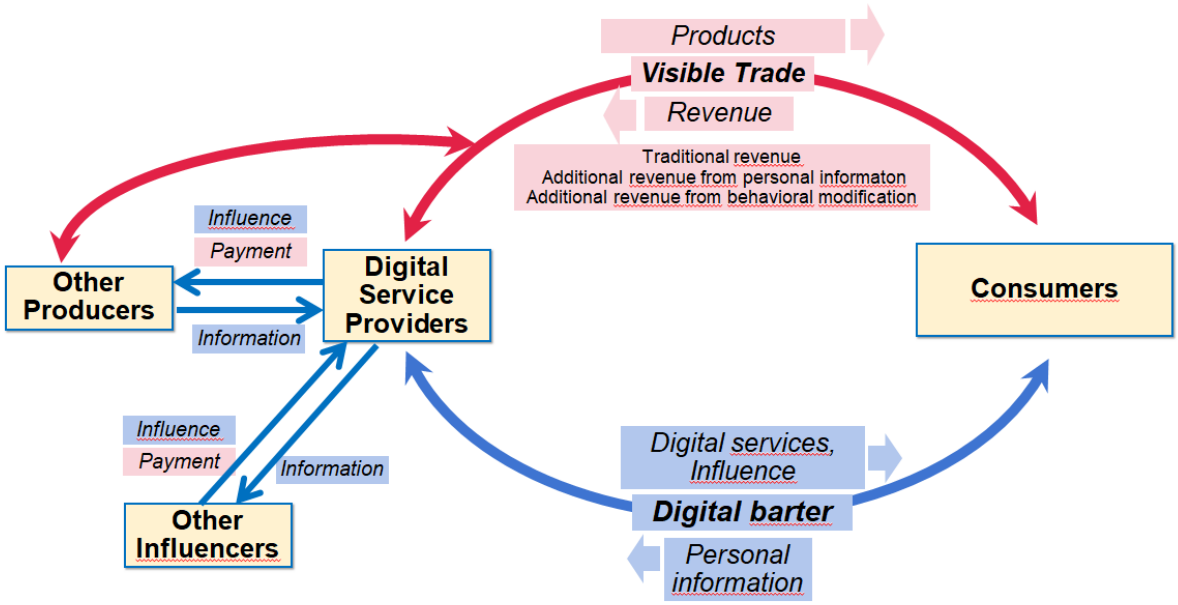

Figure 3: The Cross-Subsidization System

It is apparent that this is an elaborate system of cross-subsidization. The digital services are, of course, not free: they are compensation for the influencers' ability to extract personal information from the consumers and to exert influence on them. The influencers (traditional producers and other influencers) remunerate the digital service providers for this access. In return, the producers receive additional revenue from the personal information (allowing them to target their products more appropriately to the consumers' preferences) and the behavioural modification (allowing them to mould the consumers' preferences towards their profit-making products).

Whereas the standard economic transactions (denoted by the red arrows) are all visible (measured and counted in GDP), the digital barter transactions (denoted by the blue arrows) are invisible: the flows of free digital services, personal information and influence all take place outside economic markets and, from the perspective of the consumers, largely outside conscious awareness. As the process of digitization proliferates, the visible trade is being shaped increasingly by a growing digital "shadow domain" lying outside markets and often outside our perception and understanding.

For most people with digital access, their social, economic and political lives are conducted substantially through digital platforms, which inevitably shape their interactions with one another. By providing the tools for engaging in tasks, the interactive media become the avenues whereby people connect with one another, and provide access to new social actors. In this sense, digital technology is inherently persuasive.[5]

Though many users are aware that they are revealing information about themselves through their digital platform use, they are generally unaware of all the inferences that are drawn from this information and of the elaborate behavioural modification to which they are subject, as much of the persuasion takes place implicitly and unconsciously through the selective information content and social context generated by the platform.[6] In this sense, the current system of third-party-financed digital barter is intrinsically deceptive.

The digital users' decision-making processes are affected by the digital services through the following major channels, driven by the objectives of the digital influencers:

- *Social identity formation*: The users' social networks – underlying their social, business and political affiliations – are constrained and shaped by the digital network providers, in accordance with the objectives of the influencers.
- *Attention capture*: The digital network providers seek to capture as much of their users' attention as possible, because more attention translates straightforwardly into more opportunities for revenue from advertising and other influence selling activities.
- *Solicitation for network growth*: Digital network providers seek to induce their users to attract further users, in order to grow their digital networks. The larger the network, the more valuable it becomes to the users, and thus the more user attention it can attract. This is an important channel whereby the digital network providers shape their users' social networks.

[5] See, for example, Bogust (2007), Fogg (2002), Moon (2000), and Reeves and Nass (1996).
[6] See, for example, Oinas-Kukkonen and Harjumaa (2008).

- *Persuasion*: Digital network providers' aim to earn revenue from advertising and other persuasive activities gives rise to a natural incentive to exploit users' psychological weaknesses and thereby make them vulnerable to social, political and economic exploitation (along lines described below).

The pursuit of these four objectives means that, in effect, the users are being "farmed," in the sense that their attention, preferences, beliefs, norms, values and identities are directed and influenced for the purpose of revenue extraction. This phenomenon may be called "*digital husbandry*." In other words, digital services have become far more than an information-gathering device, enabling sellers of products to make more accurate predictions of their customers' demands. More importantly, the digital services are a goal-shaping device, whereby users' thoughts, feelings and identities are moulded in the interests of the influencers.

Digital husbandry takes place without intrinsic regard for the authenticity of personal data. Different digital service providers assemble different stores of data about each individual, creating different explanatory and predictive models of the individual, depending on the individual's digital use and the objectives of the influencers. This means that each digitally connected individual has an array of digital identities, one for each of the digital platforms that the individual uses. There is no mechanism to ensure that official personal data – that is, data whose content is uniquely authenticated by a legally accepted source (such as one's name, address, identification numbers and asset information) – is indeed in accord with its authenticated counterpart. On this account, the stores of personal data held by the digital service providers – generated by the user, by the user's interactions with other users, or by inferences from such data – need not be anchored in truthful representations. While individuals spend much time and effort to ensure the internal consistency and coherence of their physical and psychological identities, there is no mechanism that automatically respects this need in the digital arena. This lacuna provides ample latitude for disinformation and duplicity.

The system of third-party digital barter is inefficient, since the prices of the digital services do not directly reflect the value of these services to the users. The concentration of market power in the hands of the digital service providers contributes to severe inequities that create and exacerbate the economic, social and political fragmentation of many societies. Furthermore, the system also gives digital

service providers inadequate incentives to protect their users' privacy. The concentration of information on digital platforms makes the system is inherently vulnerable to cybersecurity risks. Thereby the system leads to systematic threats to a range of widely accepted human rights. On all these counts, the current digital governance regimes may undermine the economic, social and political progress that has been made throughout the world over the past three centuries.

Policy makers have repeatedly attempted to mitigate these deficiencies, for example, by giving users the opportunity to consent to cookies and to agree to terms and conditions of particular digital services. These and other constraints on the data extraction and persuasive activities of the influencers are unlikely ever to let users achieve self-determination in their digital activities. Given the huge asymmetries of information and power between most users and their digital service providers, it is difficult – generally impossible – to ensure that users are given a fair set of options from which to choose. Currently users are often confronted by cumbersome terms and conditions for the use of digital services, making it difficult to provide informed consent. Even if regulators were able to enable informed consent at present, this achievement is likely to be transient, since digital technologies continue to change rapidly and the much slower moving legal and regulatory frameworks are unlikely to keep pace. Ultimately, the digital service providers and the regulators are locked in an arms race, in which one side seeks to extract information and exert influence on the users while the other side seeks to protect the users' freedom to remain in charge of their own decisions.

The fundamental reason why regulatory efforts to defend users' rights under the current digital governance system are likely to fail is straightforward. The problem is not the misbehaviour of market participants who do not abide by the rules of the game. Instead, there is a systemic flaw in the current digital governance system that decouples the objectives of the digital service providers from those of the users. To address the problem of digital husbandry, policy makers need to correct the underlying systemic flaw.

In effect, the third-party-funded digital barter decouples economic prosperity (measured in terms of goods and services) from social prosperity (measured in terms of people's wellbeing in thriving societies). The influencers pursue their economic, social and political gains, which are not necessarily aligned with the users' authentic

needs and purposes. The users have little, if any, opportunity to signal their needs and purposes to the digital service providers, since they are locked into a system of digital barter – generating free information about themselves in return for free digital services. The provision of digital services – along with the associated goods and services in the offline world – is not driven by the goals of the users, but rather by the goals of the influencers.

To promote the wellbeing of individuals in thriving societies, economic prosperity must be recoupled with social prosperity. The self-evident way to do this is to give users control of the data that is generated about themselves, directly and indirectly, individually and collectively. This means giving individuals the right to grant or withhold personal information in accordance with their individual objectives, within the existing legal, political and social constraints. It means giving individuals the right to structure their social, economic and political networks in accordance with their collective objectives, again within the legal, political and social framework. It means creating governance systems that prevent large asymmetries of information and power.

Thereby people acquire the opportunity to benefit from economic gains from trade, social gains from affiliation, and protection from domination in their economic, social and political realms. The unprecedented economic growth experienced by the many advanced and emerging countries around the world over the past three centuries – along with the spread of economic, political and social freedoms – would have been impossible without such governance systems. This human miracle – raising living standards, reducing poverty, promoting freedom of individual and collective initiative, and generating knowledge and innovation at unprecedented scales – now needs to be achieved in the digital world.

This paper outlines three sets of policy proposals that aim to generate market conditions that pursue the objective of recoupling economic prosperity with social prosperity. These market conditions are pictured in Figure 4.

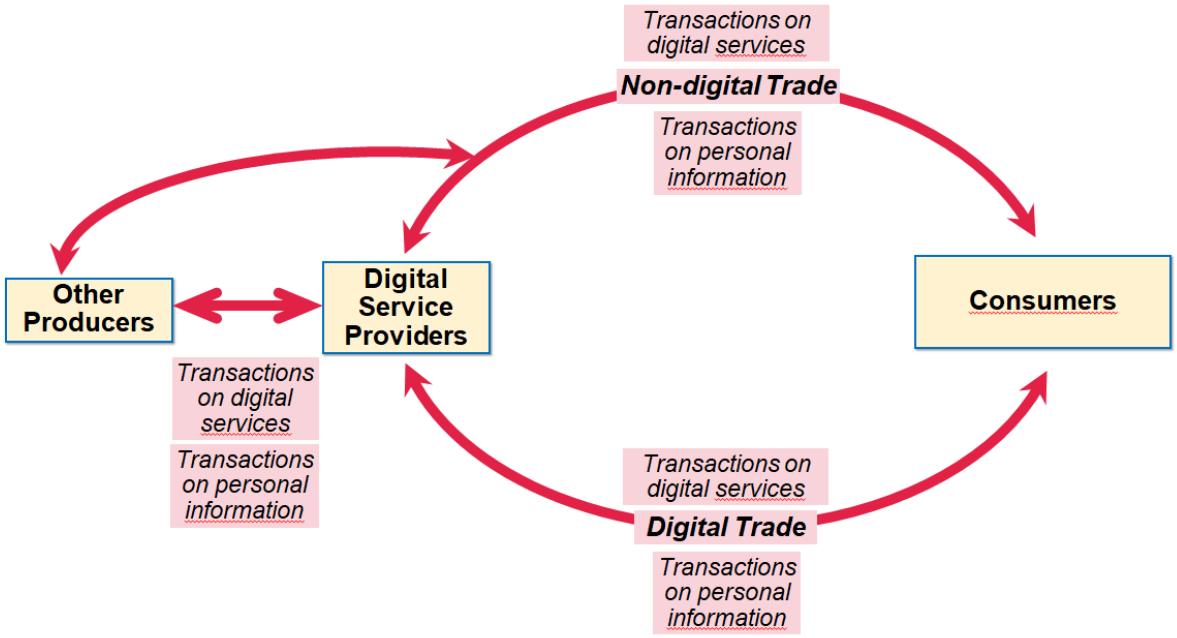

Figure 4: Towards Recoupling Economic and Social Prosperity

In the left-hand side of the figure, the producers engage in digital trade with the digital service providers, with buying and selling taking place with regard to both digital services and personal information. These transactions may involve compensation in money or in kind. The upper part of the figure depicts the non-digital trade, in which products and information are traded in return for revenue, and in the lower part of the figure, digital trade is depicted in analogous terms, again either monetary or in kind. When users have rights of association in the digital realm, the existing asymmetries of information and power may be mitigated. Note that the "shadow domain" of non-market, largely non-conscious activities (previously denoted by the blue arrows) has been eliminated. This system is not based on misunderstanding and duplicity.

The current digital governance regimes have developed along different lines from their counterparts in the offline world and many of the grave problems that threaten our economic, social and political progress have arisen on account of this governance divergence. Although digital data differs from most goods and services in the offline world, the governance divergence cannot be rationalized through this difference. While digital data is non-rival (its use by one user doesn't reduce its availability to others), there are many offline goods and services that are non-rival as well, such as public goods, club goods and common-pool resources. Many insights have been gained over the past decades concerning the appropriate governance of

non-rival offline goods and services and these insights have yet to reach the online world.

The central claim of this paper is that the benefits of the current digital regime can be retained, while the above-mentioned problems above can be mitigated through three insights. The first is a new classification system, in which personal data is divided into three distinct realms, each with distinct norms of appropriate data use. This new classification permits new policy approaches to be imagined. The second element comprises three sets of policy proposals, aimed at rectifying the deficiencies of the current governance regime, promoting economic, social and political freedoms and preventing the accretion of large power asymmetries. The third element is a set of implementation options that enable data subjects to gain appropriate control over their personal data.

Our vision of the future is one in which

- the opening up of access to and control of common data to the many will support a renewed flourishing of innovation;
- new entrants will have enriched competition in online markets where competition rules have been adapted to online dynamics;
- users will have greater understanding and confidence in the companies with whom they interact, as they have authorization, access and control of what data they share, with whom and under what conditions;
- no company will hold key information on an individual without that person’s knowledge and consent, unless as prescribed under law, for clear exceptions such as law enforcement or national security;
- attempts to influence online will be aligned with the interests of the users and efforts at disguised economic, social or political manipulation will be illegal and auditable;
- both users and companies will have confidence that key personal data collected online is dedicated to its specific purpose and is accurate, certified, up to date and auditable;
- the data collected by the Internet of Things, with either explicit, observed or referred data about the individual citizen will be guided by similar policies to

ensure that citizens are aware of and can control the collection of personal data about themselves;

- basic human rights will be upheld automatically through the incentives generated by the digital governance system; and
- freedom of association and collective bargaining will have enabled skilled agents for millions of users to negotiate for them more equal use and financial terms with large data holders.

Though the problems described above are universal, the current European personal data governance regime appears to offer the greatest opportunities for a reassessment of digital governance. Thus our proposals are of particular relevance in this governance context and seek to build on this foundation. In particular, we claim that the EU's General Data Protection Regulation (GDPR), the forthcoming e-Privacy Regulation, Digital Services Act and Data Act, along with related European regulations and laws[7] can be simplified and developed to address the problems above.

Like existing European personal data governance, the proposals in this paper recognise that all companies have become data companies and influence citizens' wellbeing though the manipulation of data. The proposals are applicable to all companies (perhaps with some limited exemptions for small businesses, similar to the GDPR) although for illustrative purposes the following pages will focus primarily on the data aggregation and platform companies.

The current European governance regime relating to personal data has significant practical problems. In particular, it exposes users to economic and political manipulation through the content and organization of information they receive through their digital tools (such as smartphones) and services (such as social media), allegedly on the basis of meaningful user consent and the "legitimate interests" of large data brokers and advertisers. Thereby the current governance system threatens to undermine systematically the ability of digital users to make free, sovereign decisions in their social, economic and political domains.

[7] We note that the European Democracy Action Plan is another locus of work for addressing some of the issues we raise in this paper. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12506-European-Democracy-Action-Plan

To address these deficiencies, we present our new classification system for personal data and then proceed to our three sets of policy proposals and their implementation.

Classification System

In our proposed new classification system, the three realms of personal data, along with their purposes, are specified as follows:

- **O-Data** – "official data," for which the content is uniquely authenticated by the state or other legally accepted source, but its control and rights to access is managed by data subjects. Examples: Name, date of birth, passport number.
- **C-Data** – "collective data," which people agree to share within a well-defined group, for collective purposes that can be defined by voluntary agreements or through law, governed by rules associated with the "data commons". Examples: Geographic data for digital maps, smart city' data, aggregated data from banking and farming cooperatives, medical research data including that of under-served groups.
- **P-Data** – "privy data," which is about individuals, but is not collective and does not require authentication. "First-party P-Data," which is volunteered or generated by individuals, is to be controlled by the people it is about. Examples: Personal blogs, autobiographical information. "Second-party P-Data," which is generated or inferred by others from existing data (e.g. profiles of people), is to be used in the interests of the people it is about. Examples: Location data from smartphones, records of a person's past purchases of goods and services.

Policy Proposals

In the context of this classification system, we make three sets of policy proposals:

- **Control over O- and P-Data:** Give individuals genuine control over use of their O- and P-Data, by enabling them to decide what data is to be provided to whom and when, supported by the appropriate technical tools and institutions. Whereas individuals are to have direct control of first-party P-Data, second-party P-Data is only be used in the interests of the people it is about. The governance of second-party P-Data is to be treated analogously to that in the offline world concerning

intimate data that is not held by the data subject, such as in doctor-patient or lawyer-client relations.

- **Control over C-Data**: Establish a range of "data commons" to allow people, instead of platforms, to manage and benefit from C-Data, both individually and collectively.
- **Addressing Power Asymmetries**: Address digital power asymmetries along the same lines as in the offline world, providing rights of association for individuals, giving legal protection to vulnerable users and ensuring online competition along the same lines as offline.

Implementation Options

Our proposals aim to mitigate these problems while retaining the wide-ranging benefits of the current digital system. The upshot of our proposals is to put control over personal data into the hands of individuals or their freely chosen social groups and to reduce the power asymmetries in digital markets. The proposals do not undermine the important benefits generated by the current digital service providers, but rather enable the users – rather than the third-party funders – drive the ongoing development of digital services.[8]

The proposed new regime is practically implementable with existing technologies. It will however need broad adoption via legal requirements. In Europe, the GDPR offers a promising foundation for such an endeavour at the EU level. It can play a central role securing the European digital single market, but is fully consistent with the GDPR.

- Enable individuals to gain control over their O- and P-Data and enable social groups to gain control over their C-Data by using institution-building strategies at the EU level and a range of technologies building on some of the the lessons of Personal Information Management Systems (PIMS), self-sovereign identity (SSI) and high scale data record query and resolution.

[8] For example, many of the most widely used digital services, such as digital maps and social networks, can be reconstituted in the form of C-Data governed by our proposals 2 and 3.

- Address digital power asymmetries by extending competition law as well as laws to safeguard the right of association and protections for vulnerable groups.
- Enable groups and communities of interest to gain control over their C-Data through the establishment and support of data-trusts, particularly data commons.

These three elements – the classification scheme, the policy proposals and the implementation options – provide an overarching framework for developing the digital governance of personal data in the EU, as summarized in Figure 5.

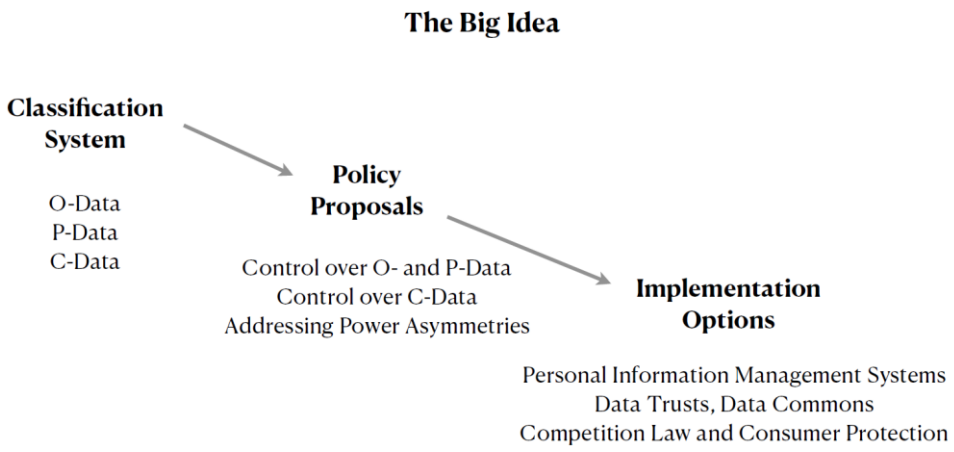

Figure 5: Recommendations

This paper is structured as follows. Section 2 surveys the deficiencies of the current digital governance regime. Section 3 articulates appropriate goals for government policy that underlie our revisit of digital governance. Section 4 presents our new classification scheme for personal digital data. Section 5 contains our digital governance proposals. Section 6 provides a cursory overview on how the proposals can be implemented. Section 7 explores some important implications of the proposals, concerning consumer protection, containment of pandemics, and taxation of digital goods and services. Finally, Section 8 concludes the paper.

2. Deficiencies of the Current Digital Governance Regime

The current regime has unleashed huge benefits for all digitally literate people. Unprecedented amounts of information have become conveniently available to countless people, at little or no cost. Goods and services can be tailored to suit users' personal needs. Countless firms are able to satisfy users' demands more efficiently than heretofore through the use of digital technologies. Staying in touch with one's communities has become much faster and more convenient than ever before. Sharing of data permits more input into AI applications, better recognition of phenomena, better forecasts of behaviour and thus improvements in the associated services.

In the light of the wide-ranging benefits from the current systems of data use and sharing, amending the digital governance regime has become an extremely sensitive topic, for two main reasons. First, it is widely feared that changes in digital governance might endanger these benefits. Second, digital service providers have accumulated massive market power that remains largely invisible in our daily digital transactions. This power is being used to protect the resulting wealth of the digital service providers, both through the provision of information to their users about their role in society and through political lobbying in favour of the current digital governance regime. While the GDPR is a world-leading instrument for the protection of personal data, there are many detailed aspects of the governance regime in practice that are so far under-developed under the case law of the Court of Justice of the EU, and in terms of institutional and technical measures needed to provide effective protection in the rapidly-moving digital markets now so central to many people's day-to-day lives.

The current European digital governance regime still suffers from the following major deficiencies,[9] most of which arise from the control of the planetary-scale advertising platforms that fund many Internet services. This 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.[10]

---

[9] For a far-reaching overview of these deficiencies, see Brown (2016).
[10] Zuboff (2019).

Many of these deficiencies also apply to the exponentially growing data being generated by the Internet of Things (IoT). More things than people are connected to the Internet, things that are constantly collecting data but which are retreating into the background context of the material world in a way that people don't even see. Yet the vast amounts of data they collect can be used to infer great degrees of information about individuals. On this account the proposals also cover IoT data.

2a. Inefficiencies

Profoundly damaging and wide-ranging inefficiencies arise inevitably from the current regime.

First and most fundamentally, the widespread use of third party-financed digital barter makes it impossible for the market system to provide incentives for economic resources to be allocated to their most productive uses in satisfying users' needs. There is no mechanism ensuring that, for every individual, the marginal value of the free Internet services is equal to the marginal value of the users' information. On the contrary, in the light of the digital service providers' immense profitability, we have reason to believe that the value of the information supplied by users to the service providers far exceeds the value of the Internet services that the users get for free.

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 in users' interests.[11] Second, the current regime is responsible for far-reaching asymmetries of information, since data subjects have little knowledge of how their data is used by the providers of digital services and third parties to whom the data may be resold. This asymmetry of information greatly reinforces the asymmetry of market power between data subjects and digital service providers, addressed below.

Third, the current regime enables the digital service providers to exploit a range of cognitive biases (including limited attention to new products, services and hardware by new market entrants; inertia; endowment effects; users' knowledge gaps due to

[11] These and other sources of inefficiency are explained in Posner and Weyl (2018).

infrequent experience of data breaches, and excessive discounting of future costs relative to immediate benefits).

Fourth, the current regime generates inefficiencies through the exploitation of a wide range of transaction costs. These include the costs of legal action in response to misuse of personal data, difficulties in assessing and proving the origins of data misuse, and the users' limitations in time, attention and skills in evaluating privacy policies and data breaches. The legal limitations are augmented by the failure of courts to recognize probabilistic or uncertain harm.

2b. Inequities

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. This exercise of market power is both inefficient (preventing entry of new providers and reducing incentives to innovate) and inequitable (promoting great concentrations of income and wealth in the hands of the data and network owners).

Since 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.

2c. Inadequate protection of privacy, by design

Digital data is non-rival: The use of data by one user does not reduce the availability of that data to others. Thus data can be used by any number of users simultaneously. Most economic analyses emphasize the benefits of data sharing, due to improvements in the allocation of resources and in the rate of innovation.[12] Some analyses recognize the importance of privacy concerns, but commonly claim that data markets are able to balance privacy concerns[13] against gains from data sharing.[14] This claim is unfounded.

For example, Acemoglu et al. (2019) argue that there are important reasons why data markets under-price individual-level data. People who share their data not only compromise their own privacy, but also the privacy of others whose data is correlated with the former data. This is an important negative externality: people do not take the full costs of their data sharing into account. Consequently there is excessive data sharing. This leads people to relinquish more of their data, giving less weight to their privacy concerns, since other people's data sharing has already revealed much about the former. Other authors have argued that, on account of market power asymmetries, users are not adequately compensated for the data that they generate.[15]

Jones and Tonetti (2020) show that when firms own the data on digital platforms, they may not only show inadequate concern for the privacy of their users but may sharply limit its use by other firms and this limitation is profoundly inefficient. In their analysis, giving users control over their data generates an allocation of resources that is close to social optimality. The reason is that the users are in a position to balance their privacy concerns against the gains from selling their data. Ali et al. (2019) also shows how the non-rivalry of information leads to the underutilization of information when firms own the data.

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

[12] For example, Varian (2009), Veldkamp et al. (2019) and Veldkamp (2019).
[13] For example, Stigler (1980), Posner (1981) and Varian (2009).
[14] For example, Laudon (1996) and Posner and Weyl (2018).
[15] For example, Ibarra et al. (2018) and Posner and Weyl (2018).

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 – 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.[16] In some cases, users have the possibility of opting out of some surveillance, but often in return for significant loss of service.[17]

2d. Exploitation of psychological weaknesses

Through the exploitation of psychological weaknesses, digital service providers under the current digital regime induce their users to behave in ways that are detrimental to their health and the achievement of their other personal goals. This happens in a variety of ways.

First, 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. The users are generally vulnerable to negativity bias and loss aversion (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.[18] This undermines their psychic health and promotes social discord.

Second, users generally suffer from 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.

---

[16] 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."

[17] 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.

[18] See, for example, Baumeister et al. (2001).

Third, the digital intermediation of much interpersonal communication through the social media tends to promote more shallow interpersonal relationships, both because direct interpersonal interactions are frequently interrupted through digital exchanges and because the large amounts of time we spent on the social media goes at the expense of direct interactions. Our concern with being "liked" in the social media leads many to spend time accumulating large numbers of social media "friends" rather cultivating unmediated personal relationships through sustained interactions in the physical world. Our emotional life, as a result, becomes more shallow.[19]

Fourth, as consequence of users' negativity bias, threat sensitivity, and digitally intermediated interactions, users are more prone to belittle, demean and bully others on social media platforms. Since the spectrum of potential disagreements among social media participants is a continuous array ranging from rationally argued, constructive criticism to bullying, the conflictual behaviour on the social media is intrinsically difficult to regulate – particularly when the users are not involved in designing the regulatory process. On account of the incentives created by third-party-financed digital barter, the social media platforms who currently control the media content have a natural tendency to err on the side of encouraging user attention, which often is often associated with aggressive behaviour.

Finally, 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

[19] See Carr (2010).

has an inflammatory influence on our brain cells, which may be linked to depression.[20]

In short, the continuous stimuli we receive through our smartphones and other digital devices hurts our concentration and makes us anxious. Our instinctive response to this 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 state of protracted distraction and interruption hurts our cognitive faculties, hurts our intelligence,[21] and harms our productivity.[22]

2e. Inadequate cybersecurity

The current regime is exposed to a variety of threats, extending across the broad domains of cybercrime (motivated by financial gain or service disruption)), cyber-attack (often involving politically motivated information acquisition) and cyber-terrorism (violence aimed at creating fear and intimidation for the purpose of political or ideological ends). Cybersecurity may be compromised by malware, phishing, SQL injections, denial-of-service attacks, man-in-the-middle attacks, and much more. The problems extend across a variety of domains, covering network security, operational security, information security, application security, disaster recovery, etc.

These problems often arise from systemic vulnerabilities (which in practice have so far only been partially addressed by the Network and Information Systems Security Directive and the Cybersecurity Act), and are growing on account of increasingly sophisticated and determined adversaries (state and non-state, including organised crime). As the danger of major cyberattacks to our medical, financial and other systems continues to grow and as international agreements concerning cybersecurity continue to lag far behind those applying to physical warfare, the mitigation of cybervulnerabilities through digital governance is of great importance.

---

[20] Bullmore (2018) examines the link between inflammation and depression.
[21] See Gazzaley and Rosen (2016).
[22] See, for example, Puranik et al. (2019) examines the effects on productivity.

2f. Threat to the proper functioning of the market system

By encouraging "third party-financed digital barter," the current regime undermines the workings of the free market system, together with the governments that rely on this system for tax revenues. The reason, obviously, is that the free market system works through price signals, which digital barter has eliminated.

Two necessary (but not sufficient) conditions for a market system to function in the interests of its participants are that (i) the participants have control over the goods they sell and gain control over the goods they buy and (ii) the participants have the opportunity to engage in voluntary exchange, by trading goods at prices that they have agreed on. The current digital regime does not give users effective control over the personal data that they supply, since this data is generally controlled by the digital service providers. Furthermore, the users do not have the opportunity to engage in voluntary exchange because, as noted, the current regime is based on the exchange of free personal information for free digital services. In this setting, the users are usually given a highly restricted choice between agreeing to the terms and conditions of this digital barter or foregoing the associated digital services. In effect, users have the choice between receiving services that are designed to maximize the returns of the digital service providers or not participating in the modern information society.

2g. Vulnerability to political manipulation

The current regime permits the digital service providers to use their wide-ranging control of digital personal data for the purpose of manipulating users' political preferences, thereby undermining democratic processes around the world. The ultimate economic and political objective that drive this manipulation are those of the third parties who fund the digital barter.[23]

It is important to emphasize that where limitations on political manipulation exist, they are self-imposed and untransparent to the users, with limited accountability on the part of the digital service providers. There are no generally accepted rules to which

[23] While Google has recently imposed limitations on political micro-targeting, and Twitter has banned political advertising, Facebook – by far the world's largest platform by reach – has steadfastly refused to do so.

users have consented, and no independent audits associated with graduated penalties for misconduct.

2h. Vulnerability to social manipulation

The revenues from advertising and other interest-selling depends on user attention. This user attention is secured most reliably through (i) highlighting threats (as humans are more sensitive to losses than gains) and (ii) connecting people to their like-minded counterparts (due to the forces of confirmation bias and social solidarity). On this account, it is not surprising that digital service providers are prone to amplifying information that promotes conflict and reinforces social segmentation. Thereby the current regimes undermine the cohesiveness of societies and political entities.

This threat to social cohesion is particularly serious since digital platforms have become essential for maintaining the social infrastructure. These platforms have become a major avenue of communication with families, religious organizations, educational communities, political movements, and many other social groups. Of particular importance in this regard are the "gatekeeper platforms" that connect the influence buyers (in the economic, social and political domains) to their potential recipients. For example, e-commerce platforms connect retailers to their customers; and social media platforms connect advertisers to users. These platforms are commonly connected to "digital ecosystems", connecting devices, networks, data sources and digital tools (such as Google Search, Google Home digital assistant, Google Pixel smartphone, Gmail, Google Meet, Google Translate, Google Calendar, Google Earth, Google Maps, Google Play, YouTube, etc.). These platforms and their ecosystems play a vital role in shaping social communities. The current governance regime puts this shaping process ultimately into the hands of the third parties funding the digital barter.

2i. Vulnerability to economic manipulation

On account of the deficiencies above, the current digital governance regime is highly vulnerable to economic manipulation. The primary source of this manipulation is third party-funded digital barter – trading digital services for information about the users of

these services at zero prices (or at least artificially low prices, subsidized by the third-party funding). This phenomenon implies that the content and organization of information that reaches the users is shaped by the objectives of the third-party funders. Since the content and organization of information is the basis on which economic decisions are made, economic manipulation is an inherent, ineradicable aspect of the current digital governance regime.

Economic decision-making rests on the perceptions, beliefs and preferences of market participants. Each of these determinants is in the hands of the digital service providers through the flow of digital information that they manage in the interests of third-party funders. This phenomenon gives new, disturbing meaning to the aphorism "The medium is the message."

This is the fundamental vulnerability to economic manipulation on which the other vulnerabilities are built. These latter vulnerabilities include the exploitation of behavioural biases and transactions costs, as well as the generation of massive asymmetries of market power.

2j. Disempowerment

The propensity of the current digital regime to provide incentives that induce digital service providers to exploit their users' psychological weaknesses and make them vulnerable to political, social and economic manipulation is not just inequitable; it is also 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 with prearranged and prefabricated by digital service providers driven by third-party funding.

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 Thinks (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.[24] 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.

2j. Threats to Fundamental Human Rights

On account of the deficiencies above, the current digital regime is systematically prone to threaten fundamental human rights, as articulated in the Charter of Fundamental Rights of the European Union:

- **Dignity**: the right to the integrity of the person (Article 2), which is systematically threatened through the proliferation of digital identities pertaining to an individual, outside the control of the data subjects (for first-party P-Data and C-Data) or the authoritative sources (for O-Data and second-party P-Data);
- **Freedom**: the right to liberty and security (Article 6), respect for private and family life (Article 7), protection of personal data (Article 8), freedom of expression and information (Article 11), freedom of assembly and of association (Article 12) and freedom to conduct a business (Article 16), which is systematically threatened through inadequate protection of privacy, inadequate cybersecurity, the exploitation of users' psychological weaknesses

[24] For an excellent account of these problems, see DeNardis (2020).

and the consequent vulnerabilities to political, social and economic manipulation, and the asymmetries of market power;

- **Equality**: The right to equality before the law (Article 20), non-discrimination (Article 21), equality between women and men (Article 23), rights of the child (Article 24), and rights of the elderly (Article 25), which is systematically threatened through intransparent use of data through the third-party funders of the digital networks;
- **Solidarity**: Workers' right to information and consultation (Article 27), right of collective bargaining and action (Article 28), right of access to placement services (Article 29), protection in the event of unjustified dismissal (Article 30), fair and just working conditions (Article 31), protection of family and professional life (Article 32), social security and social assistance (Article 33), and consumer protection (38), which is systematically threatened in the informal labor markets of the gig economy;
- **Citizens' rights**: The right of access to documents (Article 42), which is systematically threatened on account of the significant transactions costs involved in gaining such access currently.

3. Appropriate Goals for Government Policy

All the deficiencies above are associated with well-known social ills that have received significant public attention. They all need to be addressed by setting appropriate goals for government policy.

The vulnerabilities to political, social and economic manipulation are associated with disempowerment, i.e. the loss of decision-making agency. These vulnerabilities, together with inadequate protection of privacy, are also associated with the social ill of unravelling communities of interest, i.e. crumbling social solidarity. The accretions of market power generate inequities arising from vast inequalities of income, wealth, skills and employment opportunities. The inefficiencies are associated with loss of productive capacity and thereby diminished material living standards.

Appropriate goals for government policy should address this range of social ills, which extends well beyond the problems that conventional neoclassical economic analysis aims to confront. This analysis is focused on the material wellbeing of

economic agents, which arises from the consumption of goods and services. In this context, the goals of government policy collapse to the minimization of inefficiency and inequality. Inefficiency reduces the amount of output that can be produced from a given quantity of resources and thereby reduces the amount that can be consumed. Inequality in income and wealth is considered harmful because the marginal utility of consumption is assumed to fall with income and wealth, so that the wellbeing of rich people increases by less in response to a rise in income and wealth than the wellbeing of poor people decreases in response to a fall in income and wealth of equal magnitude.

This analytical framework ignores the policy goals of agency and solidarity, viewed as phenomena that are distinct from inefficiency and inequality. To understand the need for privacy and protection from manipulation, it is important to recognize that a loss of agency hurts people not just because their consumption opportunities are thereby reduced, but also because agency is itself a fundamental human need. It is also important to recognize that a loss of social solidarity hurts people not just because it reduces trust and thereby gains from trade, but also because the expression of pro-sociality is itself another fundamental human need.

The conventional economic analysis of information focuses primarily on connecting consumers with products. Consumers seek to find the products whose consumption gives them most utility and producers seek to find the consumers who are willing to pay most for their products. In this context, the disclosure of personal data leads to a rise in efficiency in the search and matching process and a resulting rise in material wellbeing from consumption (e.g. Posner (1981). Asymmetries of information associated with disclosure of personal data may however lead to efficiency losses, due to adverse selection and moral hazard (e.g. Hermelin and Katz (2006)).

These considerations ignore the need for privacy as a fundamental human right. This right has a personal dimension that is associated with human agency (the power to restrict disclosure of information about oneself to others) and a social dimension (the power to restrict disclosure of information about one’s social group to outsiders). Neither of these dimensions falls within the purview of conventional economic analysis.

For all these reasons, appropriate goals of government policy must include, but also extend beyond, the consumption of goods and services. As the success of the

human species rests largely on cooperation and niche construction,[25] we have inherited other needs from our evolutionary past, especially the need to socialize (particularly in groups of limited size) and the need to use our capacities to shape our environment.[26] These needs for solidarity and agency, alongside material wellbeing and environmental sustainability, are present in all cultures.

These needs are associated with fundamental human motives and moral values. The need for solidarity is associated with cooperative motives – such as care (seeking to promote the wellbeing of others) and affiliation (seeking belonging within social groups).[27] These motives are associated with people's sense of purpose, giving meaning to their lives, and are thereby linked to fundamental moral values, such as universalism, benevolence, and conformity, in the value circumplex of Schwartz (1994). The need for agency is associated with individualistic motives such as achievement (seeking to attain predetermined, often socially accepted, goals)[28] and status-seeking (seeking social standing and social influence)[29] and self-interested wants.[30] These motives are also related to fundamental values, such as those of power, achievement, hedonism, and self-direction in the Schwartz (1994) circumplex.

The deficiencies of the current governance regime can all be understood as obstacles to the satisfaction of these fundamental needs and purposes. For example, inadequate protection of privacy is destructive of agency and power asymmetries exert an adverse influence on both agency and solidarity.

Our classification scheme, policy proposals and implementation options, described below, are meant to improve digital governance of personal data in terms of the major government policy objectives above, covering social solidarity, personal agency, material gain, and environmental sustainability.[31] The underlying motivation

---

[25] This is the process by which an organism shapes its own environment.
[26] See, for example, Henrich (2017). While online platforms have given users innovative ways to socialize, the the shape and content of the social networks is commonly geared to revenue extraction from the users, rather than the direct expression of the users' social needs
[27] The caring motive is concerned with nurturance, compassion, and care-giving, e.g., Weinberger et al. (2010). The affiliation motive is concerned with belonging, e.g., McDougall (1932), Murray (1938), and McAdams (1980).
[28] See, for example, Atkinson and Feather (1966); Pang (2010).
[29] This motive is analysed, for example, in H. Heckhausen (1989) and J. Heckhausen (2000).
[30] This motive is covered by the individualistic preferences of neoclassical utility theory in economics.
[31] Performance in accordance with these objectives – Solidarity (S), Agency (A), material Gain (G) and Environmental sustainability (E) – is measured over a large number of countries and extended time period by SAGE dashboard of Lima de Miranda and Snower (2020).

is straightforward. Solidarity, agency, material gain and environmental sustainability are each important, separate contributors to human flourishing. They cannot be substituted for one another and are not always correlated with one another. Thus they cannot be subsumed in measures of GDP and its distribution. Consequently developments of the digital governance regime should aim to promote people's communities (solidarity to their social commons), their sense of empowerment (agency to influence their fate their own efforts), their living standards (material gain that promotes their consumption opportunities) and their ability to live within planetary boundaries (environmental sustainability within the natural commons).

4. Classification: Three Realms of Personal Data

For the purpose of formulating digital policy, it is useful to distinguish between three types of consequential personal data[32]:

O-Data is "official data" that requires authentication by third parties for the purpose of conducting legally binding transactions and fulfilling other legal obligations in many jurisdictions. Authentication can come from the state or other legally accepted sources. (Example: Name, date of birth, professional qualifications, land registry deeds.)

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.[33] C-data is subject to the same security requirements and restrictions on unpermitted onward transit as P-data currently is under data protection laws.

P-Data is data that does not require authentication by third parties and is not collective. It may be data that is volunteered by the data subjects (such as personal photographs), generated by the data subjects (such as location data from mobile phones), observed (such as a transaction) or inferred (such as psychological data deduced from web searches).

---

[32] See Annex 1 for a definition of personal data.

[33] This definition of "data commons" is not related to common pool resources, since the former is excludable while the latter is not. See Annex 1 for the place of personal data (on the one hand) in the common distinctions between private, club and public goods and common pool resources (on the other).

In the proposals on data governance that follow, these three types of data are to be governed by the following usage norms:

- O-Data is to be authenticated by the legitimate parties.
- C-Data is to be governed by the rules associated with the "data commons." This data is associated with major externalities, i.e. uncompensated effects on third parties (not involved in the relevant data transactions).[34]
- P-Data may be divided into "first-party data"[35] volunteered by the data subject or generated by the data subject and observable by other parties, and "second-party data" generated by a second party about the data subject or inferred about the data subject from existing data.[36] Data subjects are to be given effective control over first-party data, and second-party data is to be used only in the interests of the data subjects. The data subjects have the right to specify what is in their own interests. This right applies not only to unambiguous relationships of trust (such as doctor-patient) but also to other second party data, such as targeted advertising. It also applies to inferred data about the data subjects from material objects (IOT).

The types of data and norms on data use are summarized in Figure 6.

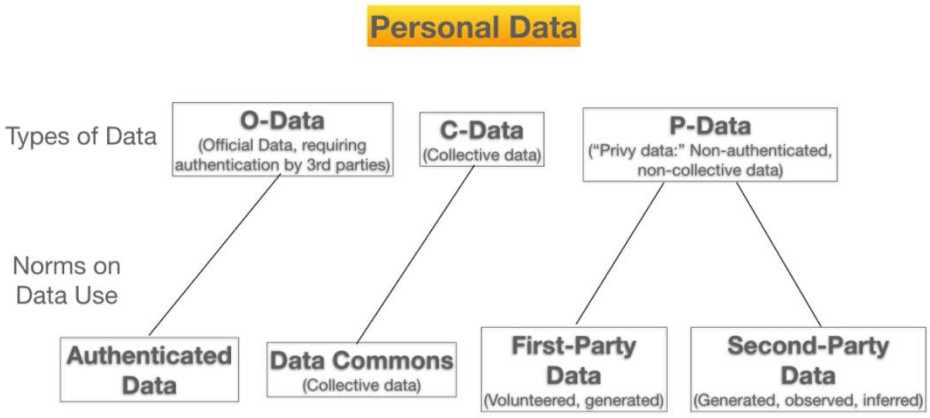

Figure 6: Types of Data and Norms on Data Use

[34] This definition of "data commons" is not related to common pool resources, since the former is excludable while the latter is not. See Annex 1 for the place of personal data (on the one hand) in the common distinctions between private, club and public goods and common pool resources (on the other).
[35] Examples: news articles, personal photographs.
[36] Example: Personality characteristics inferred from web search behaviour.

5. Proposals for Digital Governance

5a. Control over O- and P-Data

Proposal 1: Give individuals genuine control over use of their O- and P-data.

1a: Coordinate the provision of easy-to-use technical tools and supporting institutions that enable users to control the use of their O-Data. This O-Data should receive official (*Generally Trusted Source*) authentication and is to be the only legal source of this data.

Under a new legal framework, which makes this record the only way in which such data may be drawn by third parties, the data subject will have the power to allow the collection of the data by a third party and under terms set by the data subject.

The following are examples of O-Data:

- Name: full name, maiden name, mother's maiden name, or alias
- Personal identification numbers: social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number
- Personal address information: street address, or email address
- Personal telephone numbers
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting
- Biometric data: retina scans, voice signatures, or facial geometry
- Information identifying personally owned property: VIN number or title number
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person

While the content of O-Data is not controlled by data subjects (since this data requires authentication by legitimate sources), data subjects are to control and manage it. In short, 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.[37]

1b: Through the above-mentioned technical tools and supporting institutions, enable users to directly manage and control their O-Data and first-party P-Data and ensure that this data is the only legal source of this data.

Providing direct, effective control of first-party private 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. For example, in the context of competition reform, the European Parliament's Internal Market Committee has called for the European Commission to "provide consumers with technical solutions to help them control and manage flows of their personal information".[38]

Currently there are few if any laws requiring that all parties must access first-party private 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.[39] Whenever a company or other party requires this data, it

[37] 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.

[38] European Parliament, Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Legal Affairs with recommendations to the Commission on Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), 9 July 2020, §22.

[39] Our proposal does 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 identifer to get activated by the aggregator's algorithms when a particular device is 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, similarly to laws against tax evasion.

should not be inferred or observed, but be drawn from the user-controlled authoritative source.[40]

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. [41]

1c: 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).[42]

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

---

[40] 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.

[41] 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.

[42] 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.

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.

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. We would suggest 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.[43]
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 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.

This proposal also requires a reallocation of meaningful control from digital service providers to the data subjects, because only once such individual and collective control is ascribed to the data subjects can the legitimate interests of the data subjects be defined. Legal protections can be drawn from "fiduciary law" frameworks, which consider the expertise, benefit and confidences in trusted but almost definitionally imbalanced professional relationships.[44]

There is a profound, yet relatively easy to implement, step to create such a fiduciary duty for data brokers. The G20 member states and other states could make G20 AI Principles practical by extending the regulatory requirements they have for doctors,

---

[43] 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
[44] Balkin (2016).

teachers, lawyers, government agencies, and others who collect and act on individuals' intimate data to apply equally to data aggregators and their related AI implementations. Any actor who collects intimate data about an individual should be required to act on, share, or sell this data only if it is consistent with that person's interests. This would force alignment of the interests of the target/consumer/user and the firm in the position to manipulate. 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 (Balkin 2015). This would make data brokers responsible for how their products and services were used to possibly undermine individual interests.

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 goal of governance would be to make the basis of manipulation visible to the target and others, in other words, 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. Registering would be particularly important for political advertising so that researchers and regulators can identify the basis for hypertargeting. 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. Transparency and accountability online and offline could be brought into consonance with each other. In other areas, where a lawyer or realtor or financial advisor has intimate knowledge and a conflict of interest (where they could profit in a way that is detrimental to their client), they must disclose their conflict and the basis for their conflict.

5b. Control over C-Data

Proposal 2: 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.[45] 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. (This implies that the permissible uses of C-Data be clearly distinguished from those of P-Data.[46])

The data commons is a defined and protected structure to which people can delegate the stewardship of certain subsets of their data (i.e. data not included in the 'basic data-set' on citizens that governments authenticate). 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

[45] 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).

[46] C-Data may include P- and O-Data, among other things.

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.

2a: 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.

Implementation requires a reallocation of access and control rights away from those in the current digital regime and a refocusing of control and benefits towards the people data concerns and the communities and societies they inhabit. The current deficiencies point both to the anti-competitive concentration of data and its exploitation, but also to the under-provision of public data goods. As data collection and use is driven by advertising technology, less commercially exploitable but socially and economically useful forms of data are not available – for example, granular wage and salary data, large scale and longitudinal data-sets related to social equity, environmental and agricultural data. The current system may even reduce 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 anticompetitive advantage against the data subjects, for example farm and cooperative-level agricultural productivity data.[47] Finally, large-scale data-sets about the public – such as smart city data – should be

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

evaluated to assess whether both their value and the risk and consequences of misuse merit these data-sets being managed in data trusts or commons with a clear fiduciary obligation to the data subjects.

To create opportunity for a wider range of societally beneficial data-uses, this proposal is for legislative support to create minimum legal definitions (where needed), 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. As well as providing a basic 'vessel' or minimum and flexible example of the legal definition of the data commons, legislation may 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 are derived from Elinor Ostrom's Core Design Principles on the management of common pool resources.[48]

2b: Ensure that the data commons are permitted to use data only for specified purposes, managing their relationships to reduce asymmetries of power and information.

Data commons use of C-Data (and other types of O- and P- data that may be inferred from or connected to it) is subject to the transparently developed and published purposes of the commons, developed using processes modelled on Ostrom's principles, and subject to the fiduciary responsibilities of the commons management to data subjects to carry out their collective will and not cause harm. The relevant application of existing data protection law to C-data applies the existing notice and consent regime for data transfers, and also the significant requirements for ensuring the security of that data.

Key to addressing power asymmetries is actively encouraging the rights of association of data-subjects. Data commons will be encouraged as a means for

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

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 ensure that data commons act against both current and future potential power asymmetries, data interoperability[49] will be required.[50]

5c. Addressing Power Asymmetries

Proposal 3: Address digital power asymmetries along the same lines as in the offline world.

In particular, three major instruments exist offline for mitigating such asymmetries: government safeguard of the right to association, laws protecting vulnerable groups, and competition law.

3a: Provide effective rights of association for digital users.

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, in order to counterbalance the significant asymmetries of power that have developed between large online platforms and their hundreds of millions (in some cases, billions) of individual users. This could build on the notion of collective redress in the GDPR (Article 80), and political movements to improve labour protection in the so-called "gig economy",[51] as well as trade union campaigns to protect their members against disproportionate surveillance at work.

3b: Provide effective legal protection for vulnerable digital users.

---

[49] Brown, I. (2020, July 30). Interoperability as a tool for competition regulation. https://doi.org/10.31228/osf.io/fbvxd
[50] Further information about Data Commons is in Annex Four.
[51] Woodcock and Graham (2019).

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.

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. Any actor who collects intimate data about an individual should be required to act on, share, or sell this data only if it is consistent with that person's interests – and that interest cannot merely to provide more targeted advertising. 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.[52]

3c: 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

[52] 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.

the resulting power asymmetries should be treated more analogously to the regulation of natural monopolies offline.[53] 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.

In practice, while the EU's existing data protection and fundamental rights regimes are increasingly aligned via both CJEU judgments and cooperation between data protection regulators and human rights agencies,[54] greater coherence is needed between consumer protection and competition regimes (despite the efforts of the "Digital Clearinghouse" established by the European Data Protection Supervisor[55]). These regimes also need significant work to effectively incorporate social partners such as trade unions.

3d: Provide GAAP-like oversight to data traffickers with regard to the protecting the data they hold.

Governments could 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 (2018) 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.[56] 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

---

[53] For a summary of the literature on the regulation of natural monopolies, see Joskow (2007). For a recent analysis, see Ducci (2020).
[54] See, for example, Case C-311/18 -- Facebook Ireland and Schrems.
[55] See EDPS, Big Data & Digital Clearinghouse, at https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en
[56] 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.

cope with market needs while remaining responsive and protecting individual rights and concerns.

The proposals and implementations are summarized in Figure 7.

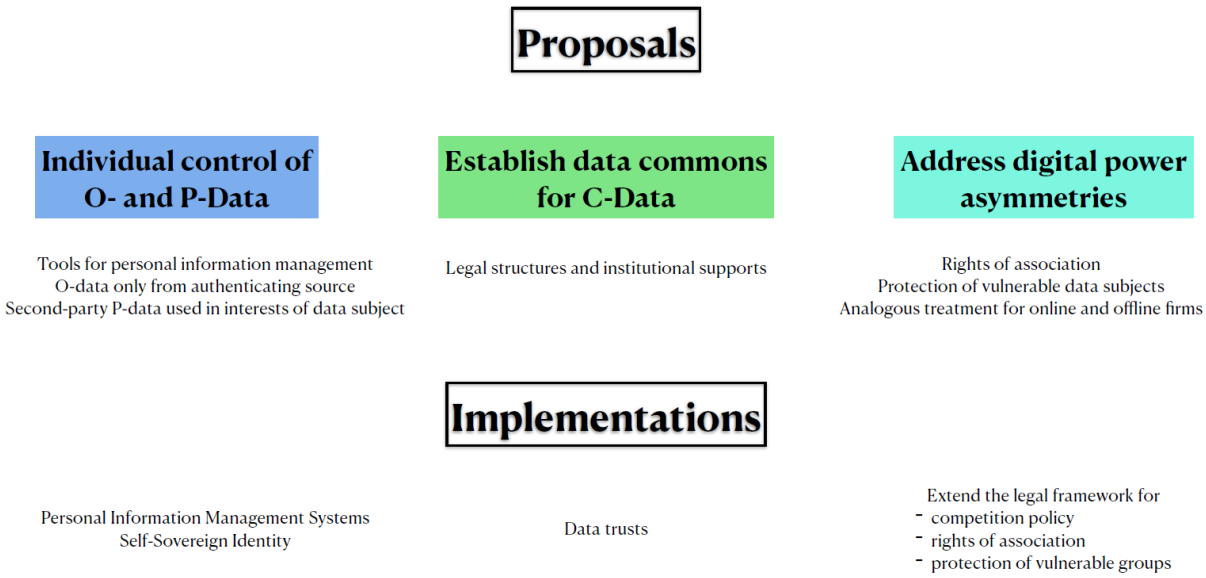

Figure 7: Proposals and Implementations

6. Implementation of the Proposals

Implementing Proposals 1a and 1b is technically not a particularly daunting task. The online economy has several examples of single sources of authenticating or downloading data. Examples include the credit card transaction and online travel booking systems.

Perhaps a more pervasive example is the Domain Name System (DNS) – the backbone “look-up table” for the Internet. Using a hierarchical and distributed set of databases, including data supplied by internet companies and consumers, it enables billions of requests from people and Internet of Things devices to be resolved - resulting in data being transferred and web sites being presented. Consider that the loading of one page of an e-commerce web site can result in more than 50 DNS requests – all of which resolve in part of a second. And that process takes place billions of times per day as the world surfs the web. This gives a sense of the scale

and robustness of the DNS. The sort of data look-up and download system we envisage supporting this policy would run on existing DNS infrastructure and processes.

While Internet's Domain Name System is a useful model for the distributed, high speed resolution of queries for authoritative data, more complex and privacy-protective technical architectures have also been developed in EU-funded research projects such as SPECIAL[57] and DECODE.[58] A further range of technologies and processes – such as aspects of self-sovereign identity systems[59] and Personal Information Management Systems (PIMS)[60] – are also relevant to the implementation of Proposals 1a and 1b.

Proposal 1 c (using second-party P-Data exclusively in the interests of the data subjects) can be implemented through laws governing integrity and confidentiality of second-party relationships, such as doctor-patient and lawyer-client, as well as the technologies above-mentioned.

The implementation of Proposal 2 requires further extension of competition law in the digital domain, along with laws safeguarding the right to association and protecting vulnerable groups. Proposal 3 can be implemented through data trusts.

These proposals are all consistent with the GDPR. Elements of these proposals are under specific consideration in the European Commission's proposed Digital Services Act and Data Act.

All these elements of implementation involve the following policy initiatives:

- support for technologies and institutions that permit people to gain control of their personal data,
- support for processes that permit responsible management of second-party personal data and the data commons, and
- legal and regulatory frameworks that permit the implementation of the three proposals above.

---

[57] See https://www.specialprivacy.eu
[58] See https://decodeproject.eu
[59] See Annex 2.
[60] See Annex 3.

In order for people to adopt technological tools that will more effectively protect their personal data, they will need public support in managing their digital identities. For example, they will need to have access to convenient digital sources of evidence for the correctness of the information they provide and receive (through digital signatures of third parties to prove authenticity),[61] procedures ensuring transparent consensus concerning the content and conduct of transactions, and systems ensuring consistent usage rights for the individual's data.

Since digital identities are meant to function across legal jurisdictions, it will be vital to specify an international legal framework relevant to each transaction. For this purpose, the EU General Data Protection Regulation (GDPR) uses the principle of Lex loci solution is, in which transactions are associated with the citizenship of the individuals involved.

The prerequisites for the establishment of the new digital regime require public support, much as governments were required to build the internet and give people access to it. But meeting these prerequisites should be easier, cheaper, and much faster than the large public efforts of the past, such as building water, rail and road networks during the Industrial Revolutions. Laws mitigating asymmetries of market power in digital markets – through appropriate extending competition law to personal data, establishing and sustaining practically effective right of association in digital markets, and protecting vulnerable groups in these markets – also requires active government involvement.

The new regime will not happen by itself. There are too many digital companies with vested interests in maintaining control over their users' data. For the new regime to become successful, it needs broad adoption. For broad adoption in the EU, it must be made a legal requirement for the EU. The new digital regime could play a central role in the creation of a European digital single market and is consistent with the GDPR. Progress on this front could put the EU at the vanguard of a new digital age in which online and offline policy becomes harmonized and the growing problems of the current digital regime are overcome.

---

[61] For details on how this can be done, see Rannenberg et al. (2015).

6a. Control of Personal Digital Data

Under the current digital regime, major digital service providers effectively control much personal data, with few effective constraints on using this data in their own interests. This allocation of control, along with the governance regime built on this basis, prevents the implementation of all the proposals above.

Thus a reallocation of control is fundamental to the development of current digital regime. First-party privy digital data has the same relevant characteristics as the private non-digital goods. In both cases, the goods are excludable and are not associated with major externalities. The fact that private digital data can be replicated at negligible marginal cost, in contrast to most offline goods, is not a reason for denying individuals their rights to control the data they generate. On this account, Proposal 1 requires that data subjects be given control over their first-party private data, and that second-party private data be used in the interests of the data subjects. This means that the second parties should act as if the data subjects were in control of their personal data, provided that they had the same information as the second parties. Proposal 2 gives individuals the effective right to associate and to counterbalance the power of large data controllers.

In the offline world sharing information with a particular market actor, such as a firm or individual, requires trust and other safeguards such as regulation, professional duties, contracts, negotiated alliances, nondisclosure agreements, etc. The point of such instruments is to share information within a (now legally binding) safe environment where the interests of the two actors are forced to be aligned. However, three facets of manipulation by data traffickers[62] strain our current mechanisms governing privacy and data. First, manipulation works by not being disclosed, thus making detection difficult and rendering the market ill-equipped to govern the behaviour. Second, the type of manipulation described herein is performed by multiple economic actors including websites/apps, trackers, data aggregators, ad networks, and customer facing websites luring in the target. Third, data traffickers –

[62] Those in a position to covertly exploit the relative vulnerabilities or weaknesses of a person in order to usurp their decision making

who collect, aggregate, and sell consumer data – are the engine of manipulation of online consumers yet have no interaction, contract, agreement with individuals.

These three facets – manipulation is deceptive, shared between actors, and not visible by individuals – render the current mechanisms ineffective in governing the behaviour or the actors. For example, Europe's General Data Protection Regulation is strained when attempting to limit a 'legitimate use' of data traffickers or data brokers who are looking to market products and services based on intimate knowledge. An individual has a right to the restriction of processing of information only when there are no legitimate grounds of the data controller. This makes GDPR fall short because legitimate interests can be broadly construed to include product placements and ads. Moreover, the manipulation of individuals has not been identified clearly enough (yet) as diminishing a human right of freedom and autonomy.

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 goal of governance would be to limit the use of intimate knowledge by making certain types of intimate knowledge either illegal or heavily governed. 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 within the AI Principles as a legal right.

Protecting personal digital autonomy involves expanding the definition of "intimate knowledge." One important step in this direction involves explicitly including inferences made about individuals as sensitive information within existing regulations such as the GDPR (Wachter and Mittelstadt 2019). Sandra Wachter and Brent Mittelstadt have recently called 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. These inferences would then be considered intimate knowledge of individuals that could be used to manipulate them (e.g., whether someone is depressed based on their online activity). The inferences data traffickers make based on a mosaic of individual information can constitute intimate knowledge about who is

vulnerable and when they are vulnerable. Current regulatory approaches only protect collected data rather than the inferences drawn about individuals based on that data.

A further step towards protecting personal autonomy involves enforcing shared responsibility. Digital service providers can be made responsible for who they partner with to track or target users. Customer-facing websites and apps should be responsible for who receives access to their users' data – whether that access is by sale or by placement of trackers and beacons on their sites. Third parties include all trackers, beacons, and those who purchase data or access to users. Websites and apps would then be held responsible for partnering with firms that abide by GDPR standards, EU or G20 AI Principles, or new standards of care in the US. Holding customer-facing firms responsible for how their partners (third-party trackers) gather and use their users' data would be similar to holding a hospital responsible for how a patient is cared for by contractors in the hospital. Or, holding a car company responsible for a third-party app in a car that tracked your movements. This would force the customer-facing firm, over whom the individual has some influence, to make sure their users' interests are being respected.[63] The shift would be to hold customer-facing firms responsible for how their partners (ad networks and media) treat their users.

Yet another step is to expand the definition of "sold" data. All regulations can include beacons and tracking companies in any capacity to notify if user data is "sold."

6b. Handling the O-Data System

The components of the proposed system are:

- authentication and hosting of the collated data,
- a legal obligation for all companies/entities to source official type data only from the citizen controlled record,
- authorization for access according to negotiated terms,
- companies implementing their initial official data request,
- companies ensuring up to date upgrades to the data, and

[63] Lauren Scholz first used the term data traffickers, rather than data brokers, to describe firms that remain hidden yet traffic in such consumer data (Scholz 2019).

- the auditing of companies to ensure the use of official data is consistent with the regime set out above.

First step is that a service provider, one of many which could be a private player or government actor, would offer citizens the facility to enter key official data records.[64] The service provider would then provide the citizen with pathways to draw **authentication** for each piece of data from the appropriate layer of government, educational institutions or other recognized bodies. This authentication would be in the form of being signed with a digital certificate issued by the authenticating body. The data can then also be signed with a digital certificate issued by the service provider. These signatures ensure a digital "paper trail" as to the authenticity of the records and where the authentic copy is stored.

As an added protection against possible political manipulation of authorization in a sub-jurisdiction, the European Commission could also establish an institution to sign the government certificates (and implicitly audit the certificate authorities at the sub-jurisdictional level).

This general approach of citizens filling in such types of data and ensuing authentication from approved bodies is similar to one already taken by banks or other financial institutions in the offline world – under the purview of national supervisory authorities ensuing that the AML/KYC process is followed correctly.

Thus at the authentication stage, the key to governance is not who holds the data record but the accumulation of specific digital certification.

The function of the service provider outlined here is built on capabilities already well established in the existing ICT infrastructure. For instance, the role of helping a user collate some required data and then holding that data securely, but allowing approved access and transfer of data in very short time is similar in scope and capabilities of DNS registries. Considering that the proposed system is supported by governmental or other recognized trusted bodies for authentication, a distributed and fast transacting data base system will better service the technical and policy requirements than a relatively slow and expensive transaction on a blockchain system.

---

[64] Exactly what should be included needs more consultation but could include name, address, personal identification numbers, personal characteristics, and biometric data.

Another reason for preferring a data base system, capable of authorized amendment, rather than an immutable blockchain is the need for some flexibility in specific fields to enable people to maintain autonomy and not be unduly constrained by the record – for instance flexibility in the address record for people who are homeless, displaced persons or refugees, people at threat of domestic violence or in the midst of changing addresses. The ability to say "no" to a party requesting such data is an important right to ensure that the citizen controls the use of this data.[65]

Further, it will be important to require that the access to these official data fields does not contribute to algorithmic discrimination especially for the purposes of employment, provision of governmental, financial, medical, educational, housing, social or other key services. The legal framework establishing the approach to data governance suggested in this paper would do well to establish specific legal implementation of Artificial Intelligence and Algorithmic ethics as outlined recently, especially the principles for responsible stewardship of trustworthy AI agreed by the G20 in 2019. The correct governance for AI and its underlying Big Data has been discussed at national and dispersed international fora for several years, including efforts by the Council of Europe[66], the Innovation Ministers of the G7[67], the European Parliament [68], and the Organisation for Economic Co-operation and Development (OECD)[69]. In June 2019, the Group of 20 (G20) Trade Ministers and Digital Economy Ministers adopted a set of AI Principles[70] that draw from the OECD's principles and discussion of proposals from G20 engagement groups[71]. These principles point to a more human-focused and ethical approach for guiding AI.

---

[65] But as the GDPR has prescribed (including the right to be forgotten) there will also need to be some flexibility in the entries in some of the official information fields to manage for the edge cases.

[66] https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10

[67] https://g7.gc.ca/en/g7-presidency/themes/preparing-jobs-future/g7-ministerial-meeting/chairs-summary/annex-b/

[68] Directorate-General for Parliamentary Research Services (European Parliament), A governance framework for algorithmic accountability and transparency. Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf

[69] https://www.oecd.org/going-digital/ai/principles/

[70] Annex to G20 Ministerial Statement on Trade and Digital Economy. Available at https://www.mofa.go.jp/files/000486596.pdf

[71] For instance, see Paul Twomey, "Building on the Hamburg Statement and the G20 Roadmap for Digitalization: Toward a G20 framework for artificial intelligence in the workplace." Available at https://www.g20-insights.org/policy_briefs/building-on-the-hamburg-statement-and-the-g20-roadmap-for-digitalization-towards-a-g20-framework-for-artificial-intelligence-in-the-workplace/

The second principle is **obligation**. Just as in off-line rules for the use of identity cards for various transactions/interactions (e.g. checking into a hotel) in the member states of the European Union, we propose a new legal obligation for all companies/entities looking to collect and/or store official type data only be able legally to source it from the citizen controlled record with the digital certificates we mention above. This builds on the obligation already established in the GDPR for all companies to know where they hold personally identifying information on individuals and what data they hold and to share with the individuals the purposes for processing their personal data, the retention periods for that personal data, and with whom it will be shared. The new obligation suggested here requires that the companies only source the data from the authenticated records held on behalf of the citizen. While this would be an auditable regulatory requirement, it brings one big benefit to business not provided by the GDPR: the authenticated status of the data will be a significant boon in diminishing the risk of fraud by potential customers, vendors and employees.

To ensure that companies are able to prove to auditors that they have sourced the O data only from the authenticated records held by the individual's selected service provider, it would be important for the service provider to digitally water mark or fingerprint the record to say from where the record has come. This would be additional to the layers of digital certification outlined above. The legal structure to support this obligation would also require entities which receive O type data from another source not to use it and to report the source to authorities (similar to the regime concerning receiving stolen property).

The follow on stage is **authorization** – who has the right to access these records and on what terms. Here is the crux of re-empowering the citizens to ensure 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. Again, 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. The agent could be the service provider who holds the record or be a separate entity which

negotiates on behalf of the citizen and informs the service provider of the terms for access. Such a two tiered market has echoes in the off-line economy. For example, some people choose to place their retirement savings in full service pension funds while others use an investment platform to gain access to a range of specialist investments/funds managers/strategies that may not normally be available to retail investors. 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.

While some service providers' individuals may want to approve each request for data, others may utilise a model already provided by some browsers for cookie approval of pre-setting the types of requests which will be automatically approved and others which will be refused or accepted only under certain terms.

This new arena for collective bargaining could attract law firms, mutual funds or cooperatives, trade unions or consumer unions or for-profit companies. In practice, there could be a range of people seeking to be a citizen's agent.

As well as the agent, the individual will also be able to use the record (with a specific fingerprint) for online authentication if required for credit card approvals or individual-initiated online transactions or commencements of a relationships with a company. The Individual's preferred financial and data use terms could be linked to the fingerprint.

The **initial implementation** of gaining such authorization by most companies would be straightforward. Similar to what they did during the GDPR implementation period, they would email or otherwise message their customers asking them to nominate their official data service provider and seek permission for accessing the official data. Or when they were engaging a customer for the first time, they would request the official data fields to be completed from their nominated official data service provider. The digitally signed data would be transferred to the requesting company from the data service provider together with an attached transaction-specific electronic contract certificate outlining the terms of contract agreed for the use of the data.[72]

[72] For more discussion of electronic contract certificates see https://www.fullcertificate.com/certified-electronic-contracts/

Such electronic contact certificates are already used in the real estate, trading and labour services markets in Europe.

The benefits of the transaction-specific electronic contract certificate are that it provides:

- a machine-readable format for easy distribution and implementation of instructions and conditions across a company's existing software systems and data bases.
- an auditable record of what official data can be accessed, how it may be used and by whom;
- a disincentive to sideway selling of the access to the official records to other entities or for other purposes; and
- a diminishment of the end market for, and value of, any official record stolen by a cyber-criminal from a citizen, or service provider as the value for any end user is mostly in the transaction specific authorized use terms and certification, not the personal information itself.

For companies/entities which have collated their official data type information about an individual through scraped, inferred or observed data, this new legal requirement would mean that they will have to identify specifically the individual and find who is their nominated service provider – and then seek the sort of approval and transfer of the authenticated and authorised record as outlined above. While such companies have supposedly undertaken such identification and notification of individuals under the GDPR provisions, this new process will again give the citizen clear notice of who is trying to collect data on them – but more importantly now give them the opportunity to refuse that such data be collected or set conditions (including financial conditions) under which it is collected.

Once official data has been incorporated into the systems of a company, there needs be a legal requirement to ensure on some regular basis that the data and its related permissions are up to date. The **updates** process is an area where DNS analogies may again help. To enable an optimum balance between efficiency and accuracy, the DNS requires a Time To Live process which ensures that the holder of cached data has to check regularly against the authoritative record to see if there has been any

change – and if so, to update the changed data. This sort of experience could also be applied for the official data process.

The company's systems would regularly ask the service provider's servers, Has this information changed? If the information has changed since the last time they asked, then they download the new version (although the user may have the ability to limit updates for some fields for certain interlocutors with whom they do not wish to have a continuing relationship)[73]. There are multiple ways in which such processes have been expressed technically in the past years. One could be that the service provider marks each data field with a hash of the date stamp for the information. The company servers regularly check the hash with the hash they have from the previous download. Only when the hash is different is that field downloaded as an update. This approach could also be useful for audit purposes because it can simplify the "has the correct official data been accessed and downloaded" by not necessarily checking all the data and certificates but by comparing the hashes in the company's records and those in the service provider's.

Audit of the official data being held by companies would be an essential mechanism to enforce the legal obligation for all companies/entities to source official type data only from the citizen controlled record. The auditors could conduct such checks and report on them in their reports during regular external auditor reviews of companies/entities. While auditors may need some more training to ensure they can analyze if the use of official data is consistent with the regime set out above, auditing firms have access to a computer literate workforce for the role. Indeed, with AI replacing many traditional accounting tasks, such data regime auditing could represent a growth opportunity for accounting firms.

To summarise, the business process and technical approach presented here supplements AML/KYC and GDPR and expands from data accuracy and privacy maintenance to include citizen control and benefits from their data.

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

[73] If a person gave a company permission to access her home address a couple of years ago and then moved, she may not be willing to have the company access the new home address now.

(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.

6c. Management of the Data Commons

A personal data commons refers to personal data that is associated major externalities, such as data on Covid-19 infections and immunity. Thus the membership of a data commons must depend on the magnitude of these externalities. In other words, the personal-data-driven externalities among the members of the data commons must be substantially higher than the externalities between members and non-members.

Furthermore, the members of the data commons must all be aware that they share a common purpose, on which account they are willing to join the data commons. Thus the membership of a data commons must also depend on the members' ability to forge a common sense of community and identity with respect to their common purpose.

Governments need to collaboratively set the minimum rules to create enough certainty and structure for many data commons to emerge. This will mean working cooperatively to define a range of purposes, flexible structures, decision-making abilities, liability and access regimes which data commons can adopt. The role of government is key; sufficient structure and certainty are needed to backstop the organisational structures people can innovate within, and also to ensure data is used for agreed purposes.[74] Data commons' allow people to use their rights of association

[74] Sanfilippo, et al. (2018).

to collectively assert control over their data and also, where appropriate, to generate analysis in the form of public goods.

In addition to fulfilling the need for currently under-provided “data or the public good” described above, different types of data commons will include;

- Data commons established by, for examples, trade unions or other large membership organisations, to harness large datasets of both members and non-members who may be interested, and license their use to collectively generate income for data-subjects;[75]
- Data commons established by groups currently under-served in public policy, for example, the data-gathering and analysis currently done by and for Native American tribes under-served by the US federal government;[76]
- Data commons that include longitudinal and medical data about sufferers and carriers of genetic diseases (some genetic diseases are so rare, their datasets are essentially family groups)

There is already a widely researched literature on how current data-gathering practices and structures amplify and exacerbate existing inequalities.[77] Encouraging the development of data commons will directly address this growing inequality by allowing people whose data is used to benefit from it and are not harmed from its dissemination, helping to ensure a level playing field for research and development, and incentivising the creation of standardised and usable data-sets – particularly in currently under-served groups and communities.

Data commons are a means to need to ensure citizens, groups and society at large can benefit from the use of their data, and also to productively redirect the financial value of commodified personal data back into national and regional economies. The

---

[75] We anticipate the licensing and use by peak organisations of “consent champions” – specialist templates for suggesting and manging preference profiles of individuals, developed by subject matter experts, for example, HIV advocacy bodies who have expertise and experience managing both sharing and privacy in relation to sensitive personal data. The “consent champion” concept has been developed by Anouk Rouhaak and Josh McKenty; https://www.centerfordigitalcommons.org/privacy/consent/2019/06/24/consent-champions.html

[76] https://www.uihi.org/projects/covid/ https://www.politico.com/news/2020/06/11/native-american-coronavirus-data-314527

[77] Noble (2018) and Criado Perez (2019).

goal of the data commons is not to restrict data, but to generate and distribute it in ways that maximise the benefits to the people the data concerns. Data commons' work to maximise the productive potential of data for the societies that generate it; "… if information has more value as a common resource than a privately held one, it should be held in the information commons."[78]

The management of the data commons should proceed under the same principles as those relevant for the effective management of the commons in the offline world. Regarding the latter, Ostrom's Eight Core Design Principles can serve as a useful guideline to ensure that individual and collective interests are balanced appropriately, ensuring that individuals support the commons under the presumption that their own and the collective interests are complementary to one another. These principles also ensure that the scale of the data commons (in terms of its membership) is appropriately defined and that different data commons cooperate in exploiting synergies among them.

Ostrom's Principles may be applied to the data commons as follows:

(i) Each data commons should be defined by a clearly articulated purpose, supported by a shared identity of the data commons users.

(ii) The contributions to and benefits from the data commons must be equitably distributed among the users.

(iii) The decisions concerning the management of the data commons should be fair and inclusive in the eyes of the users.

(iv) User behaviour should be monitored.

(v) Helpful and unhelpful behaviours should be met by graduated rewards and graduated punishments, respectively.

(vi) Fair and fast conflict resolution mechanisms should be available to the users.

(vii) The decision-making authority of the users must be respected by third parties.

---

[78] O'Shea (2019).

(viii) Where there are synergies to be exploited across different data commons, collaborative relations among different data commons should be promoted through polycentric governance.

A defined legal basis is needed to create the conditions for multiple data commons to emerge and flourish. Governments have already legislated in the offline world to provide the formal association frameworks for a healthy civil society to develop. Appropriate legal and regulatory structures manage risk and ensure that myriad groups, clubs, associations, non-profits, sports clubs, charities, political parties, cooperatives, mutual aid societies etc. are faithful to their founding purposes. A similar effort is needed to adapt the legal framework within which different kinds of data commons will develop.

Data commons are a key part of this proposal because they:

- restore agency to people regarding how their data is circulated and used – recognising that people often have a range of desires that include but are not limited to the commercial sphere,
- help to increase the amount and quality of data potentially available to all firms, not just the largest technology platforms, to build a more level playing field, boosting competition in line with Europe's competitiveness, values and fundamental rights, and
- are a gateway to alternative models not just to the use of data, but to secure the future flourishing of the digital economy in ways that do not rely on advertising technology, with all its inherent risks and harms.

6d. Building on Existing Security Standards

Securing how the three types of user data is stored, accessed, and transmitted is not a new problem to be solved. It is easily accomplished with existing technologies and standards. The difference is providing the user greater control in this process. These standards also include third party policy and technology audits to ensure compliance. We would recommend that the results of these audits should be sent to users who have their data stored with any of these companies. Combining these standards and applying them as a whole to companies that store user data is critical to maintaining the security of it.

All data centers storing user data will need to be SOC-2[79] and GDPR compliant. This requires data centers to establish and follow strict information security policies and procedures, encompassing the security, availability, processing, integrity, and confidentiality and privacy of user data.

Guidance and instructions on how to store and manage user data can be gained from NIST Special Publication 800-122-Guide to Protecting the Confidentiality of Personally Identifiable information (PII)[80] and the European General Data Protection Regulation (GDPR). PII is any data that can be used to identify a specific individual to include government identifier numbers, mailing or email addresses, phone numbers, IP address, login IDs, geolocation, biometric, and behavioral data. These examples provide a clear connection to user data as defined by O-, C-, and P-Data. In addition to the guidance on PII, when storing user data that contains medical information, the GDPR and HIPAA[81] standards provide laws on how to secure protected health information (PHI), or patient health data (medical records).

The Payment Card Industry (PCI) compliance model is another source for guidance on securing user data. PCI mandates credit card companies to help ensure the security of credit card transactions in the payment industry. Translating credit card transactions to the user data access processing, much of the PCI compliance can be applied. PCI compliance also outlines requirements for encrypted internet transactions, a significant concern when securing user data. Another take away on the PCI model is how it has been implemented in the credit card payment industry. Due to the strict requirements to maintain the security of transmitting and storing of credit card data, most commercial entities that process credit card payments do not have the funds nor want the responsibility of meeting PCI compliance. As a result, specialist companies have developed and maintained data centers that meet PCI compliance and specialize in these transactions. These companies provide a passthrough for the commercial entities to process the credit card transaction on their

---

[79] A SOC 2 audit reports information and confidence about a service organisation's security, availability, processing integrity, confidentiality and/or privacy controls, based on their compliance with the American Institute of Certified Public Accountants Trust Services Criteria. See https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

[80] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[81] The US Health Insurance Portability and Accountability Act of 1996

behalf. This model can also be applied to user data transactions we outline in this paper. This would create a new industry of companies that specialized in meeting the standards described above for storage and processing of user data.

7. Implications

The proposals above have far-reaching implications. The following are a sample.

7a. Consumer Protection

Under the current regime of data governance, most personal data is controlled by the digital service providers that generate and manage digital identities along with associated digital services. These firms, such as the 'Big Five' (Apple, Facebook, Amazon, Google, and Microsoft), also include data brokers, advertising networks, and data backbone contractors to governments.

The data collection industry is not new. Data brokers like Acxiom and ChoicePoint have been aggregating consumer addresses, phone numbers, buying habits, and more from offline sources and selling them to advertisers and political parties for decades. However, the Internet has transformed this process. Users rarely comprehend the scope and intimacy of the data collection or the purposes for which it is sold and used.

One reason for this is that much of the data is collected in a non-transparent way and primarily in a manner that people would not consider covered by contractual relationships. Many Internet users, at least in developed countries, have some understanding that the search and e-commerce engines collect data about what sites they have visited, and that this data is used to help tailor advertising to them. However, most have little idea of just how extensive this commercial surveillance is.[82]

A recent study of 1 million web sites showed that nearly all of them allow third-party web trackers and cookies to collect user data to track information such as page usage, purchase amounts, and browsing habits. Trackers send personally identifiable

[82] A recent analysis of the terms and conditions of the big US platforms shows that they collect 490 different types of data about each user. (See the publicly available data at https://mappingdataflows.com/ .)

information such as usernames, addresses, emails, and spending details. The latter allow data aggregators to then de-anonymize much of the data they collect (Englehardt and Narayanan 2016; Libert 2015).

However, cookies are only one mechanism used to collect data about individuals. Both little known data aggregators and big platforms collect huge amounts of information from cell towers, the devices themselves, many of the third-party apps running on a user's device, and Wi-Fi access, as well as public data sources and third-party data brokers.

Users provide their data free, in exchange for provision of digital services. The providers consequently effectively control many aspects of the users' digital identities. When/if users leave a digital service provider, they must leave all the information they generated about themselves in the possession of the provider, except (for EU residents, and users of EU-established services, under the GDPR "data portability" right) a limited subset of data that may be transferred.[83] Furthermore, the digital service providers continue to process information about former or even non-users where these users interact digitally with third parties whose digital identities are controlled by these providers. The resulting information system is inherently vulnerable to political, economic and social manipulation.

A long-standing tenet of public policy in both advanced and emerging economies is that where an economic actor is in a position to manipulate users – through the content and organization of knowledge, thereby usurping the users' decision-making capabilities – society requires a realignment of economic with personal and social interests. Individuals in some relationships – for example between religious leaders-followers, lawyers-clients, doctors-patients, teachers-students, and therapists-patients – are vulnerable to manipulation through the intimate data collected by the dominant actor, and these types of relationships are governed such that the potential manipulator is expected to act in accordance with the interests of the vulnerable party. We regularly govern manipulation that undermines choice, such as when negotiating contracts under duress or undue influence, or when contractors act in

[83] Personal data that individuals have directly contributed, or data observed by the provider, processed by the user's consent or to fulfill a contract — GDPR Art. 20(1). So far, this regime has not in practice been a success in increasing effective control by users. See, for example, Wong and Henderson (2019).

bad faith, opportunistically, or unconscionably. The laws in most countries void such contracts, and the EU has a consumer protection law framework partly addressing these issues. The digitization of information has vastly enlarged the domain of potential manipulation, since digital service providers shape the information available to individual users.

When manipulation works, the target's decision making is usurped to pursue the interests of the manipulator, outside the target's awareness. Some commentators rightly compare manipulation to coercion (Susser, Roessler, and Nissenbaum 2019). Offline, we regulate manipulation similar to the way we regulate coercion and fraud: to protect consumer choice-as-consent and preserve the autonomy of the individual.

Digital service providers, such as data aggregators, data brokers, and ad networks, can not only predict what we want and how badly we need it, but can also leverage knowledge about when an individual is vulnerable to making decisions in the interest of the firm. Recent advances in hyper-targeted marketing allows firms to generate leads, tailor search results, place content, and develop advertising based on a detailed picture of their target. Aggregated data on individuals' concerns, dreams, contacts, locations, and behaviours allows marketers to predict what consumers should want and how to best sell to them. It allows firms to predict moods, personality, stress levels, health issues, etc. – and potentially use that information to shape the decisions of consumers.

The proposals above outline an infrastructure whereby can be protected from the dangers above.

7b. Containment of Pandemics

Contact-tracing and risk-tracing technologies could help ease the 'health–wealth trade-off' confronting many countries in the wake of COVID-19. But privacy and security concerns are preventing such technologies from being widely adopted.

'Contact tracing' involves identifying people who may have come into contact, directly or indirectly, with an infected person. The contacts of infected people can then be tested for infection; those infected can be isolated and treated; their contacts can be traced, and so on (Galeotti et al. 2020). Implementing contact-tracing would greatly reduce the need for social distancing, particularly if contact-tracing were

supplemented by ‘risk tracing’, which involves dividing people into risk categories on the basis of readily available information, such as age, occupation, residence, workplace, and pre-existing health conditions (Mesnard and Seabright 2020). The effectiveness of contact- and risk-tracing can be enhanced significantly through the application of AI technologies in areas such as early warnings, tracking and prediction, visualisation, diagnosis and prognosis, monitoring crowds, and treatment support (e.g. Vaishya et al. 2020).

For countries where contact and risk tracing is feasible, people are generally willing to provide the requisite data in return for protection from infection, with three provisos: that others do the same, that their data are used only for the purpose of containing the pandemic, and that their data are adequately protected from hacking and malicious use.

In order for contact and risk tracing to become manageable in countries with significant infection rates, it needs to be done automatically through digital technologies rather than through personal interviews. Apple and Google have partnered to assist in contact-tracing through a system that includes application programming interfaces (APIs) and operating system-level technology. These companies also plan to offer a Bluetooth-based contact-tracing platform “that would allow more individuals to participate, if they choose to opt in, as well as enable interaction with a broader ecosystem of apps and government health authorities” (Government Technology 2020). The opt-in condition is meant to overcome privacy and security concerns. As Apple and Google emphasise, “privacy, transparency and consent are of utmost importance in this effort” (Apple 2020).

But the opt-in condition is expected to limit severely the uptake of this system. Opt-in policies produce far lower participation rates than opt-out policies in a wide variety of settings, from organ donations to pensions. This is so for a variety of well-known reasons: changing the default requires mental effort; the default is usually considered the preferable or acceptable choice; and people are more sensitive to losses than to gains relative to the default, making them more likely to retain the default. Governments and businesses are increasingly using opt-out design to promote socially desirable outcomes in many domains though not, as noted, in pandemic containment (e.g. Johnson and Goldstein 2003, Sunstein 2017, Thaler and Sunstein 2008). Needless to say, contact tracing software is effective only when it is widely

deployed. The system only has a high chance of detecting when a person in the system has been in contact with an infected person if a large proportion of the population has signal-emitting devices.

The opt-in policy of Apple and Google with respect to their contact-tracing app stands in stark contrast to their standard policy with regard to the use of private data for advertising purposes, as well as derivative digital strategies designed to attract user attention.

In practice, electronic devices, especially smartphones, can be understood as surveillance devices, used by network providers and app providers (such as Amazon, Apple, Facebook, Google, Microsoft, and others) to target advertising individually to users. These users are implied to have consented to this surveillance by agreeing to the digital services' terms and conditions, which they rarely attempt to read and which they would be unable to read (with all hyperlinks to other relevant documents) even if they wished to, due to the time, skill and effort required.[84] In some cases, users have the possibility of opting out of some surveillance, but often in return for significant loss of service.

Currently, most people are highly sensitive to the potential misuse of their data with regard to contact tracing, but remain largely unaware that their smartphones are de facto surveillance devices for advertising and attention-capturing purposes. Since the digital network providers earn their incomes from pursuing these purposes, they have a natural incentive to keep this asymmetric awareness intact.

Apple, Google, and other digital network providers' sensitivity to privacy and security concerns in contact tracing is understandable.

If people are given control over the use of their personal data and if power asymmetries were addressed in the online world analogously to the offline world, then these people would be more willing to make relevant data about themselves available for contact and risk tracing. After all, data trust could enable people to ensure that their data are used only for specified purposes and that they regain control over their data again as soon as the pandemic is over.

---

[84] Facebook recently offered advertisers the ability to targets teens when they are 'psychologically vulnerable.'

Furthermore, once people have control over their private data, it becomes far easier to deliberate publicly through democratic processes about the circumstances under which data is submitted to the data commons. The dividing line between private and social objectives becomes easier to draw.

7c. Taxation of Digital Goods and Services

Electronic goods and services are subject to Value Added Tax (VAT) in the EU. Businesses located in the EU are obliged to collect VAT on their sales and remit the tax proceeds to the authorities, having deducted the VAT paid on their input purchases.

Some of the problems concerning the taxation of digital goods and services are summarized, for example, in European Parliament (2016):

“While the digital economy does not create Base Erosion and Profit Shifting (BEPS) issues, it ‘exacerbates the existing ones’. Digital goods are highly mobile or intangible, physical presence of a company in the market country is often not needed in the digital sector, rendering it substantially different from traditional brick-and mortar businesses. New digital business models (subscription, access or advertisement models) and new technologies such as robotics or 3D printing are not confined by national boundaries and can easily escape their tax liabilities by channeling their royalty payments towards a tax haven, for instance.

“Taxation of e-commerce is problematic due to anonymity, difficulty to determine the amount of tax, lack of paper trail, tax havens, companies incurring liability in multiple countries, tax administration’s lack of capacity to identify companies and to manage VAT. These factors render it difficult for tax administrations to collect Value-Added Tax (VAT), especially due to BEPS risks stemming from exemptions for imports of low valued goods and remote digital supplies to consumers.” (p.8)

The proposals above address these tax challenges, since they potentially enable governments to establish the national locations of the data subjects. The proposals also create markets in information, thereby providing the possibility of levying income taxes and payroll taxes in these markets.

8. 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, bridging current digital divides, and steer technological developments in humane directions. Nevertheless, the proposals above would constitute an important step towards promoting market efficiency, reducing inequalities, enhancing protection of privacy, and promoting cybersecurity. Above all, the proposals aim to mitigate digital husbandry and thereby promote the fundamental liberties that are essential for human wellbeing in empowering and socially cohesive communities.

There are various channels whereby the proposals aim to achieve these ends.

First, giving individuals control over their O- and P-Data would create markets in these domains and thereby enable the price system to generate incentives for data provision and data manipulation, promoting economic efficiency through all the well-known channels, both in static terms (gains in matching existing supplies and demands) and dynamic terms (gains in the acquisition of human and physical capital).

Second, individual control over O- and P-Data also permits addressing digital power asymmetries analogously to those in the offline world, thereby mitigating existing inequities.

Third, individual control over O- and P-Data, along with support for the establishment of data commons, would significantly enhance the enforcement of data protection rights.

Fourth, the use of O-Data and associated use of P- and C-Data would significantly reduce a wide variety of cybersecurity threats.

Fifth, the proposals would eliminate the current system of “third-party-financed digital barter” and thereby prevent undermining of the free market system in the allocation and distribution of resources. Thereby the proposals would provide new avenues for ensuring consumer protection, implementing a wider range of digital taxation schemes, and containing pandemics and other collective action initiatives.

Sixth, by giving individuals control over O- and P-Data and giving the relevant groups control over C-Data, the digital regimes would become far less vulnerable to political, social and economic manipulation. Clearly, if users has direct control of first-party P-Data and indirect control of second-party P-Data and if the C-Data is set up in accordance with Ostrom's Core Design Principles (as outlined in the paper), then the users will not exploit their own psychological weaknesses and other agents will not be in a position to do so either.

Finally, the combination of the three sets of proposals would become a straightforward and powerful bulwark against threats to fundamental human rights in the digital realm, including the rights to the integrity of the person, non-discrimination, equality before the law, protection of personal spaces, association, consultation, and access to documents.

Annex 1: Concepts and Definitions

According to Article 4(1) of the GDPR, **personal data** is "any information relating to an identified or identifiable natural person ('data subject')." An **identifiable natural person** "is one who can be identified, directly or indirectly, in particular by reference to an identifier…" In this context, personal data is about the ability to attribute a piece of information to a person. This means that whether a particular type of information is classified as "personal data" depends on the context of the personal data in the dataset and an entity's ability to use the data to link to a person.

The economic characteristics of digital personal data may be identified in relation to those of other goods through the properties of rivalry and excludability. A good is "rivalrous" in consumption if one individual's consumption of the good reduces the opportunity for other individuals to consume the good. A good is "excludable" in consumption if those individuals who have not acquired rights over the good (such as through payment) can be excluded from consuming the good. In standard economic terminology, **private goods** are rivalrous and excludable (e.g. food and clothing); **common pool resources** are rivalrous and non-excludable (e.g. fish stocks and timber); **club goods** are non-rivalrous and excludable (such as satellite TV and private parks); and **public goods** are non-rivalrous and non-excludable (such as national defence and climate action).

	Excludable	Non-excludable
Rivalrous	**Private goods**	**Common pool resources**
Non-rivalrous	**Club goods**	**Public goods**

Table 1: Types of Goods

In this context, personal data are club goods, since they can be replicated at negligible cost and it is possible to exclude data users from access to them. The literature on efficient pricing of club goods and efficient club size[85] is of limited relevance to personal data, since the provision of the latter does not lead to congestion (i.e. a rising degree of rivalry).

Annex 2: Self-Sovereign Identities

All the proposals above can be understood in terms of a reallocation of sovereignty concerning digital identities. A **digital identity** is information about an entity (for example, an individual) that represents that entity. The digital identity arises from the use of personal information and the actions of individuals in the digital space.

A digital **identity provider** gives each user an **identifier** (often a password) in a specific domain that proves that identifies the user. Currently, identity providers focus on those user characteristics that are relevant to the identity providers' objectives, without independent regard to the user's objectives. These identifying characteristics belong to the identity provider, not to the user. Consequently, users wind up with a large number of digital identities (online personas) at various different identity providers.

A '**self-sovereign identity**' (SSI) enables users to create and control their digital identities, including unique identifiers and other identity data. Self-sovereign identities

[85] See, for example, Buchanan (1965) and Cornes and Sandler (1996).

can be implemented through decentralised ledger applications such as blockchain (which verify the accuracy of one's data decentrally, as it does for Bitcoin), although "permissioned blockchains' often take certain functions off-chain for calculation and storage in traditional data bases connected to a node.

The blockchain functionality is described below, although a blockchain implementation of the type of universal processes for a community of 450 million people proposed here would be unprecedented. To date blockchain have not been selected for such scale implementations because of issues (real or perceived) around the speed of computation and resolution, the scale of the number of transactions undertaken, and the energy cost per transaction. Networked databases has been the more traditional choice for such a large, distributed system.

A **distributed ledger** is a public ledger of transactions or contracts that are maintained in decentralized form across locations and individuals. Thus a central authority is not needed to authenticate the transactions or contracts. A **blockchain** is a list of records ("blocks") that are cryptographically linked in a public data base ("chain"). The blocks store information about the transactions or contracts and the parties to these transactions or contracts. Each block stores a unique code ("hash") enabling it to be distinguished from all other blocks. Thereby these transactions can be recorded in a publicly verifiable and permanent way.

Blockchain networks can be divided into three broad categories. **Public blockchains** are publicly transparent and fully decentralized, promoting trustworthy transactions but making it difficult if not impossible to preserve privacy in accordance with GDPR. **Private blockchains** are centralized, allowing the network operators to change entries on the blockchain, permitting operators to promote privacy but making it difficult for data subjects to have trustworthy control over their personal data (and limiting the benefits somewhat of distributed ledgers compared to higher-performance trusted distributed databases). **Permissioned blockchains**[86] allow particular behaviours and levels of access for each category of participants, promoting trustworthy transactions and making it possible to preserve privacy. This feature makes them appropriate for the SSI required for the reallocation of control over personal data. The security of permissioned ledgers depends on the integrity of

[86] See, for example, Sharma (2019).

its permissioned members, though this danger can be mitigated through smart contracts.

Smart contracts[87] are programs or transaction protocols that automatically document, execute or control actions in accordance with the terms of the contracts. These reduce the need for trusted intermediaries, arbitrators, enforcers and cybersecurity experts.

Under an SSI operating under permissioned blockchains and smart contracts, each person receives the digital equivalent of a wallet that contains verified pieces of his or her digital identity. Specifically, it gives each person a private key for an unlimited number of recipients, who can access the encrypted data only if they possess the corresponding public key. The person can then choose which identification to share, with whom and when. This makes the person 'sovereign' over his digital identity.[88]

In order for individuals to use their SSI to engage in legal, trustworthy and accountable transactions, the relevant personal data for these transactions in their digital identities should be persistent, portable, interoperable, transparent and secure. **Persistence** enables digital identities to be long-lived, for as long as the user chooses, within legal constraints. **Portability** ensures that information and services concerning digital identities are transportable, independently of third-party entities, thereby enabling the users to remain in control of their digital identities. **Interoperability** ensures that digital identities are widely usable, across technical, legal and national boundaries. **Transparency** requires that the systems that administer and operate each network of identities must be open in terms of their functioning and management. **Security** requires that digital identities they pass requirements of privacy, trustworthiness and protection. '**Privacy**' means that only authorised recipients can access a user's digital identity; '**trustworthiness**' means that the information contained in the user's digital identity is correct; '**protection**' means that the rights of the data subjects are protected, i.e. in case of conflict, the network should err on the side of the data subjects' interests over the interests of the network.

---

[87] See, for example, Fries and Paal (2019) and Savelyev (2016).
[88] For excellent summaries, see Der et al. 2017 and Tobin and Reed 2017.

Within a SSI system, each person has a unique individual digital identity (**uniqueness**) – in contrast to the current system, in which individuals possess multiple digital identities, corresponding to their multiple engagements with digital networks. Users have **control** over their identities, within legal constraints. This ensures the continued validity of their identities and, where relevant, the validity of its claims. Furthermore, users always have **access** to their data. The sharing of private data must occur only with the direct or indirect informed **consent** of the data subjects, within legal constraints. The default in consent-based data sharing should be **minimisation**, i.e. the disclosure of claims should involve the minimal amount of data necessary to accomplish the aims of the transaction.

Under these conditions it is possible to give data subjects control over their personal data, thereby enabling first-party private data to be governed by the same principles as private offline and permitting second-party private data to be used exclusively in the interests of the data subjects.

Annex 3: Personal Information Management Systems

The following background is useful for understanding the role of PIMS and SSIs in reforming governance of the digital realm.

Personal Information Management Systems (PIMS), and the related concept of Personal Data Stores (PDS), are technical mechanisms proposed to improve the portability and interoperability of systems using personal data. This should reduce switching costs and make multi-homing easier.

A PIMS gives a user the ability to manage all of their personal data, wherever it is stored, using standardised protocols and schemas to communicate with the systems holding the data. With an understanding of the meaning of that data, users can then query it in a unified way, for example asking for a recommendation for a business lunch location based on all of the user's previous lunch spots, today's weather, and any special offers available. The data may be held in one location controlled by the user, or queried directly with service providers.

A Personal Data Store lets a user store all their own personal data, whether on a device they directly control, or a remote service where the data is protected using encryption and related technical measures. The user may then authorise other

services they wish to use to interact with their own data store remotely. Solid is one project developing such tools, co-founded by the inventor of the Web, Tim Berners-Lee.

In some implementations, such as Databox, those services send software to the PDS, to run in a protected “sandbox” environment, which means the service provider never needs to access the data directly itself, thus enabling very high levels of protection for even very sensitive information.

A review by the UK’s Competition and Markets Authority identified the following potential benefits of PIMS and PDS:

1. Enable individuals to track all the users of their personal data (data controllers, in GDPR terms), and exercise their GDPR rights -- e.g. manage and revoke consent for specific uses, make subject access and portability requests, object to certain processing, and to erase data.
2. Act as identity providers, enabling an individual to log in to many different websites while protecting their privacy.
3. Act as a secure backup of users’ personal data.
4. Facilitate micropayments for services that require it, in addition or as an alternative to providing access to personal data for advertising and other purposes.

The CMA also concluded “inferred or derived data is an important factor contributing to the market power or SMS of the major platforms. Consequently, if the data sharing requirements of GDPR do not extend to derived or inferred information it may not be adequate to address our concerns.”[89]

These types of mechanisms have worked well in the UK’s Open Banking programme. The CMA found their practicability will “hinge on their commercial viability arising from consumers’ incentive to adopt them rather than their technical feasibility. That said, to work reliably such remedies may require a lot of investment in technology, including in the ancillary measures needed to support them.” These include building consumer trust in potentially unfamiliar services.

---

[89] CMA, fn , p.L12.

As with all multi-sided markets, “a prospective PIM provider would still face a difficult ‘chicken and egg’ problem: consumers would be unlikely to sign up unless advertiser-funded incentives were available but advertisers would be unlikely to use a PIMS until sufficient customers had joined.” And these cross-side network effects would tend to result in winner-takes-most dynamics, so further measures would be needed to prevent PIMS becoming a competitive bottleneck.

The Finnish government has supported the development of a MyData framework implementing a personal information management system. The framework principles are shown in Table 1.[90]

1. Human centric control and privacy: Individuals are empowered actors, not passive targets, in the management of their personal lives both online and offline – they have the right and practical means to manage their data and privacy.
2. Usable data: It is essential that personal data is technically easy to access and use – it is accessible in machine readable open formats via secure, standardized APIs (Application Programming Interfaces). MyData is a way to convert data from closed silos into an important, reusable resource. It can be used to create new services which help individuals to manage their lives. The providers of these services can create new business models and economic growth to the society.
3. Open business environment: Shared MyData infrastructure enables decentralized management of personal data, improves interoperability, makes it easier for companies to comply with tightening data protection regulations, and allows individuals to change service providers without proprietary data lock-ins.

Table 2: The MyData framework principles

There are now national MyData hubs in 40 countries, with nearly 100 organisational members of MyData Global.

[90] A Poikola, K Kuikkaniemi and H Honko, MyData – A Nordic Model for human-centered personal data management and processing, Finnish Ministry of Transport and Communications, undated, ISBN: 978-952-243-455-5.

Annex 4: Data Commons and Data Trusts

There is currently a lack of "bottom up empowerment structures"[91] for data subjects to assert their rights in a data system marked by asymmetry of knowledge and power. Rather than trying to convince people to trust current data structures, we should be working to make ones that warrant people's trust.[92] The full societal benefits of data are not achieved by purely commercial exploitation. Individually, there are many situations in which we want to share our data, both for our own and collective interests. For example, many people have unmet altruistic desires to share their data for public research – especially in healthcare – to better serve specific or marginalised communities, or to improve policymaking. However, many people have low levels of trust that data they share altruistically will be used only for the purposes it is collected, and fear that health data in particular may be commercially exploited in ways that do not recognise and reward its public value.

Examples of data that could be managed by a data commons to produce necessary but currently under-provided public goods include:

- Energy and other utility usage data currently collected by frequently non-interoperable 'smart meters' and exploited by the specific suppliers. This data could be managed instead by data commons and directed at research and better policy making on climate change.
- Location data of motorists, cyclists, pedestrians is currently considered the property of mobile operators and is commercially accessed by private firms including billboard advertisers,[93] while remaining unaffordable for most local governments to use it to improve transport, housing, education or other policies, or combine it with other data-pools to reduce hidden inequalities in existing service provision.[94]

---

[91] Delacrois and Lawrence (2018)
[92] O'Hara, (2019)
[93] https://www.ft.com/content/e5c5a996-8d54-4d5c-a5df-a036b5579148
[94] Several Swedish data studies discovered that snow-ploughing concentrated on major traffic routes rather than residential footpaths significantly increased the rate of injuries due to falls, but previous failures to disaggregate gender data had meant the snow-ploughing policy favoured predominantly male travel patterns (driving) over womens' (walking). Criado Perez, Caroline, 'Invisible Women: Exposing Data Bias in a World Designed for Men' Chatto & Windus, 2019 Data commons are a key way to plug gender data and other gaps such as this that result in policies which unintentionally exacerbate inequality.

- Sufficiently detailed salary and other employment data related to educational attainment, gender, race, etc. is currently unavailable to most people and organisations, but could be accessed widely and anonymously through data commons' to better identify and tackle biases and inequality.
- "Data for the public good", i.e. data produced by the public sector, is currently largely unavailable for use by researchers, other public sector organisations, SMEs or start-ups. Data commons could be an appropriately independent structure to make this data preferentially accessible to those groups, as recommended by the European Commission's digital strategy.[95]

There is a growing movement for individuals to assert property rights over digital data related to them. While this approach has an immediate appeal – especially in more individualist cultures – it creates more problems than it solves. Individual data property rights will vary wildly, depending on the economic status of the person, and are costly to enforce. The result is likely to be poorer people selling their data – for less money – because they need to, converting privacy from a fundamental right into a luxury good. Yet this trend – and the related drive to create tools for individuals to take control of their data[96] – captures a growing sense that the windfall profits of monopolistic technology platforms may reflect an under-valuing of personal data at scale.[97]

A **data trust** is a legal structure that provides independent and fiduciary stewardship of data. It applies the concept of a legal trust to data.[98]

Civic trusts[99] are a type of data trust that creates a trustee organization owning code and data generated by people using particular technologies and licenses them to companies that sell them. Both parties have a fiduciary responsibility to develop participatory governance structures.

---

[95] Communication from the Commission; A European strategy for data, Brussels, 19.2.20, COM(2020) 66 final, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf N.B. Although the strategy recommends making "data for the public good" preferentially available to these groups, and recommends exploring data commons in general, it does not explicitly recommend using commons for this purpose.
[96] https://mydata.org, https://radicalxchange.org, https://decodeproject.eu,
[97] Tirole, 2020
[98] The uses of data trusts are described, for example, in Edwards (2011).
[99] See, for example, McDonald and Pocaro (2015).

The connection between Ostrom's management of the commons and data trusts is clarified in Wyle and McDonald (2018).

Data commons and data trusts are of increasing interest to policymakers and others:

- Germany's data ethics commission and the Commission 'Competition Law 4.0' have both recommended the exploration of data trusts.[100] The 'Competition Law 4.0'[101] Commission also recommended the introduction of legal instruments at the European level to promote the emergence of 'trusted data intermediaries'.
- Trusted data intermediaries have been proposed – on an individual basis – by the head of competition law policy at the German Federal Ministry for Economic Affairs and Energy, as a way to counter-balance 'super-dominant digital platforms' by giving European companies similar access to data.[102]
- The European Commission's communication described "personal data cooperatives or trusts" as emerging options that "have significant potential and need a supportive environment".
- Companies such as Ericsson and Microsoft are actively exploring the use of data trusts.[103]

References

Acemoglu, Daron, Ali Mahkdoumi, Azarakhsh Malekian, Asuman Ozdaglar (2019), "Too Much Data: Prices and Inefficiencies in Data Markets," NBER Working Paper No. 26296, https://www.nber.org/papers/w26296

Ali, S. Nageeb, Ayal Chen-Zion and Erik Lillethun (2020), "Reselling Information," Computer Science and Game Theory, submitted 3 April, https://arxiv.org/abs/2004.01788v1

---

[100] https://www.stiftung-nv.de/en/publication/designing-data-trusts-why-we-need-test-consumer-data-trusts-now

[101] https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?__blob=publicationFile&v=3

[102] https://voxeu.org/article/promoting-competition-platform-ecosystems

[103] https://www.ericsson.com/en/blog/2018/3/data-commons--a-trust-framework

Allen, C (2016), *The Path to Self-Sovereign Identities*, www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Arrieta-Ibarra, Imanol, Leonard Goff, Diego Jiménez-Hernández, Jaron Lanier and E. Glen Weyl (2018), „Should We Treat Data as Labor? Moving Beyond 'Free'," American Economic Review, Papers and Proceedings, vol 108, May, 38-42.

Atkinson, J. W., and N. T. Feather. 1966. A Theory of Achievement Motivation. New York: Wiley.

Balkin, Jack M. (2016) Information Fiduciaries and the First Amendment, 49 U.C.D. L. Rev. 1183.

Blankertz, Aline, 'Designing Data Trusts; Why We Need to Test Consumer Data Trusts Now', Stiftung Neue Verantwortung, February 2020, https://www.stiftung-nv.de/en/publication/designing-data-trusts-why-we-need-test-consumer-data-trusts-now

Bogust, I. (2007), *Persuasive Games: The Expressive Power of Videogames*, Cambridge, MA: MIT Press.

Brown, Ian (2016), "The Economics of Privacy, Data Protection and Surveillance," in Handbook on the Economics of the Internet, ed. by J.M. Bauer and M. Latzer, Elgaronline, https://doi.org/10.4337/9780857939852.

Brown, I. (2020, July 30). Interoperability as a tool for competition regulation. https://doi.org/10.31228/osf.io/fbvxd

Buchanan, James M. (1965), "An Economic Theory of Clubs", *Economica*, New Series, Vol. 32, No. 125, pp. 1-14.

Bullmore, Edward (2018), The Inflamed Mind, London: Picador.

Carr, Nicholas (2010), The Shallows: What the Internet is Doing to Our Brains, New York: Atlantic Books.

Cornes, Richard and Todd Sandler (1996), *The Theory of Externalities, Public Goods and Club Goods*, Cambridge University Press, 2nd ed., pp. 347-356.

Criado Perez, Caroline, 2019. Invisible Women: Exposing Data Bias in a World Designed for Men, Chatto & Windus.

Delacroix, Sylvie and Lawrence, Neil, "Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance", (2018). International Data Privacy Law:

Doi.org/10.1093/idpl/ipz014, Available at SSRN: https://ssrn.com/abstract=3265315 or http://dx.doi.org/10.2139/ssrn.3265315

DeNardis, Laura (2020), The Internet in Everything, New Haven: Yale University Press, forthcoming.

Der, U, S Jähnlichen and J Sürmeli (2017), "Self-sovereign Identity: Opportunities and Challenges for the Digital Revolution", *Computers and Society*, Cornell University Library. https://arxiv.org/abs/1712.01767

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

Edwards**,** Lilian (2004), "The Problem with Privacy," International Review of Law Computers & Technology, Vol. 18, No. 3, pp. 263-294, November**,** https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1857536

Englehardt, Steven, and Arvind Narayanan. 2016. "Online Tracking: A 1-Million-Site Measurement and Analysis." http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

European Parliament (2016), *Tax Challenges in the Digital Economy*, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/579002/IPOL_STU%282016%29579002_EN.pdf

Federal Ministry of Economic Affairs and Energy, 'A new competition framework for the digital economy; Report by the Commission 'Competition Law 4.0'', https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?__blob=publicationFile&v=3

Fogg, B.J. (2002), *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufman.

Fries, Martin, and Boris Paal, *Smart Contracts* (in German). Mohr Siebeck. ISBN 978-3-16-156911-1.

G20 Principles on Artificial Intelligence. 2019. https://g20.org/en/media/Documents/G20SS_PR_First Digital Economy Taskforce Meeting_EN.pdfand http://www.g20.utoronto.ca/2019/2019-g20-trade.html

Galeotti, A, P Surico and J Steiner (2020), "The Value of Testing", VoxEU.org, 23 April.

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

Grossman, Robert L., Allison Heath, Mark Murphy, Maria Patterson, and Walt Wells (2016), "A Case for Data Commons," Comput Sci Eng., Sep-Oct; 18(5): 10–20, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5636009/#:~:text=available%20to%20researchers.-,Data%20Commons,resource%20for%20the%20research%20community.

Hardinges, Jack, "Data Trusts in 2020", Open Data Institute, https://theodi.org/article/data-trusts-in-2020/

Heckhausen, H. 1989. Motivation und Handlung. Berlin: Springer.

Heckhausen, J. 2000. "Evolutionary Perspectives on Human Motivation." American Behavioral Scientist 43 (6): 1015–1029.

Henrich, Joseph (2016), *The Secret of Our Success*, Princeton: Princeton University Press.

Hermelin and Katz (2006), "Privacy, property rights and efficiency: The economics of privacy as secrecy," *Quantative Marketing and Economics,* **4,** 209–239. https://doi.org/10.1007/s11129-005-9004-7

Johnson, E J and D G Goldstein (2003), "Do defaults save lives?", Science, 302: 1338-1339.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

Jones, Charles I., and Christopher Tonetti (2020), "Nonrivalry and the Economics of Data," American Economic Review, 110(9), 2819-2858. https://doi.org/aer. 20191330

Kaeseburg, Thorsten, 'Promoting Competition in Platform Ecosystems', Vox EU, December 2019, https://voxeu.org/article/promoting-competition-platform-ecosystems

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/

Laudon, K.C. (1996), “Markets and Privacy,” Communications of the ACM, 39(9), 92-104.

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

Maryam Farboodi, Roxana Mihet, Thomas Philippon, and Veldkamp, Laura (2019), “Big Data and Firm Dynamics,” American Economic Review, Papers and Proceedings, 109, 38-42. https://www.aeaweb.org/articles?id=10.1257/pandp.20191001

McAdams, D. P. 1980. “A Thematic Coding System for the Intimacy Motive.” Journal of Research in Personality 14 (4): 413–432.

McDonald, Sean, and Keith Pocaro (2015), Toward (a) Civic Trust, Medium, June 17, https://medium.com/@McDapper/toward-a-civic-trust-e3265768dfe6

McDougall, W. (1932), The Energies of Men. London: Methuen.

McGeveran, William. 2018. “The Duty of Data Security.” *Minn. L. Rev.* 103: 1135.

Mesnard, A and P Seabright (2020), “Easing Lockdown – Digital Applications Can Help,” VoxEU.org, 1 May.

Moon, Y. (2000), “Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers,” Journal of Consumer Research, 26(4), 323-339.

Murray, H.A. 1938. Explorations in Personality. New York: Oxford University Press.

Noble, Safiya Umoja, 2018. ‘Algorithms of Oppression: How Search Engines Reinforce Racism’, NYU Press.

O’Hara, Kieron, “Data Trust: Ethics, Architecture and Governance for Trustworthy Data Stewardship” (2010) Web Science Institute White Papers, https://eprints.soton.ac.uk/428276/1/WSI_White_Paper_1.pdf

Oinas-Kukkonen, Harri, and Marya Harjumaa (2008), “A Systematic Framework for Designing and Evaluating Persuasive Systems,” Proceedings of Persuasive Technology: Third International Conference, p. 164-176. https://www.springer.com/gp/book/9783540685005

O’Shea, Lizzie, 2019. Future Histories: What Ada Lovelace, Tom Pain and the Paris Commune Can Teach Us about Digital Technology, Verso.

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

Pang, J. S. 2010. “The Achievement Motive: A Review of Theory and Assessment of Achievement, Hope of Success, and Fear of Failure.” In Implicit Motives edited by O. Schultheiss and J. Brunstein, 30–71. Oxford: Oxford University Press.

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

Posner, R.A. (1981), “The Economics of Privacy,” American Economic Review, 71(2), 405-409.

Posner, Richard A. (1981), “The Economics of Privacy,” The American Economic Review, Vol. 71, No. 2, Papers and Proceedings (May), pp. 405-409. https://www.jstor.org/stable/1815754

Puranic, 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

Reeves, B., and C. Nass (1996), The Media Equation: How people treat computers, television and the new media like real people and places, Cambridge, UK: Cambridge University Press.

Roy F. Baumeister, 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.

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

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

Sanfilippo, Madelyn, Brett Frischman and Katharine Standburg, “Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework,” Journal of Information Policy, 2018, Vol. 8 (2018), pp. 116-166, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3546349

Savelyev, Alexander (2016), “Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law,” Higher School of Economics Research Paper No. WP BRP 71/LAW/2016, December, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241

Scholz, Lauren Henry. 2019. “Privacy Remedies.” *Indiana Law Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3159746.

Schwartz, S. 1994. “Are There Universal Aspects in the Structure and Content of Human Values?” Journal of Social Issues 50 (4): 19–45.

Sharma, Toshendra K. (2019), “Permissioned and Permissionless Blockchains: A Comprehensive Guide,” *Blockchain Council*, https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/

Stigler, G.J. (1980), “An Introduction to Privacy in Economics and Politics,” Journal of Legal Studies, 9(4), 623-644.

Sunstein, C R (2017), “Default Rules Are Better Than Active Choosing (Often)”, Trends in Cognitive Sciences, doi:10.1016/j.tics.2017.05.003.

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. “Technology, Autonomy, and Manipulation.” *Internet Policy Review* 8 (2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3420747

Thaler, R H and C Sunstein (2008), Nudge: Improving decisions about health, wealth, and happines, New Haven, CT: Yale University Press.

Tobin, A. and D. Reed (2017), “The Inevitable rise of Self-Sovereign Identity,” Sovrin Foundation, https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/

Twomey, Paul, and Martin, Kirsten (2020), “*A Step To Implementing The G20 Principles On Artificial Intelligence: Ensuring Data Aggregators And Ai Firms Operate*

In The Interests Of Data Subjects", Think 20 Policy Proposal, Saudi Arabia Think 20 Secretariat.

Twomey, Paul (2018), *Toward a G20 Framework for Artificial Intelligence in the Workplace,* Center for International Governance Innovation, CIGI Papers No. 178 — July 2018

Vaishya, R, M Javaid, I H Kahn and A Haleem (2020), "Artificial Intelligence Applications for Covid-19 Pandemic," Diabetes & Metabolic Syndrome: Clinical Research & Reviews 14(4): 337-339.

Varian H.R. (2009) Economic Aspects of Personal Privacy. In: Lehr W., Pupillo L. (eds) Internet Policy and Economics. Springer, Boston, MA. https://doi.org/10.1007/b104899_7

Veldkamp, Laura, and Cindy Chung (2019), "Data and the aggregate Economy," mimeo, https://www0.gsb.columbia.edu/faculty/lveldkamp/papers/JEL_MacroDataLV_v7.pdf

Wachter, Sandra, and Brent Mittelstadt. 2019. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review. 2019 (2)*

Weinberger, J., T. Cotler, and D. Fishman. 2010. "The Duality of Affiliative Motivation." In Implicit Motives edited by O. Schultheiss and J. Brunstein. Oxford: Oxford University Press

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

Wong, J., and T, Henderson (2019), "The Right to Data Portability in practice, International Data Privacy Law," doi 10.1093/idpl/ipz008

Woodcock, J. and Graham, M. 2019. The Gig Economy: A Critical Introduction. Cambridge: Polity.

Wylie, Bianca, and Sean McDonald (2018), "What Is a Data Trust?" October 9, Centre of International Governance Innovation, https://www.cigionline.org/articles/what-data-trust

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