GIDE Global Initiative for Digital Empowerment

Empowering Digital Citizens

Making humane markets work in the digital age

Dennis J. Snower and
Paul D. Twomey

GLOBAL SOLUTIONS
THE WORLD POLICY FORUM

THE NEW INSTITUTE

Empowering Digital Citizens

Making humane markets work in the digital age

Dennis J. Snower and
Paul D. Twomey

28 March 2022

GIDE is a self-selecting international group of researchers, policy experts, civil society advocates, Internet technical and security experts and businesspeople. They seek to bring new practical policy solutions and diverse international partners to ensure that the rules of the digital economy are more directed to the broad interests of humans, not just businesses and governments. Our human-centred model is beyond mere user concerns, but rather is directed to all humans (including non-users) and seeks to improve their well-being not just through material gain but also in optimising their social solidarity, agency, and environmental sustainability. The GIDE mission is to progress a model of digital governance devoted to human welfare through practically deliverable policy suggestions for pivotal policy makers.

The GIDE membership has been fortunate to have two homes. The members of GIDE are the core of the Digital Governance Program at THE NEW INSTITUTE. Founded in Hamburg in 2020, THE NEW INSTITUTE is a platform for shaping social change and to find answers to the most pressing ecological, economic and political challenges of our time. The Global Solutions Initiative has supported online meetings of the GIDE members. It is the key avenue for promoting GIDE work to the organs of the Group of 7 and Group of 20.

This report emerged from nearly two years of research and discussion by the evolving membership of GIDE. The lead authors of the report are the two Co-Chairs of GIDE: Dennis Snower and Paul Twomey. Other members and friends of the process contributed substantive text to the drafting. The GIDE membership reviewed the draft texts online and added key input through online email lists and regular online group video seminars. While the co-leads held the pen, this report is a joint effort.

Professor Dennis J. Snower is Co-Chair of the Global Initiative for Digital Empowerment and is the director for the Socio-Economic Transformation programme at THE NEW INSTITUTE. He is founder and President of the Global Solutions Initiative; Professor of Macroeconomics and Sustainability at the Hertie School, Berlin; Senior Research Fellow at the Blavatnik School of Government, Oxford; and Non-resident Fellow of the Brookings Institution. He was formerly President of the Kiel Institute for the World Economy and is Research Fellow at the Centre for Economic Policy Research (London), at IZA (Institute for the Future of Work, Bonn), and CESifo (Munich). He holds a BA and MA from New College, Oxford, and an MA and PhD from Princeton University. He has published extensively on employment policy, the design of welfare systems, caring economics and monetary and fiscal policy.

Dr. Paul Twomey is Co-Chair of the Global Initiative for Digital Empowerment and Fellow and Initiative Director for Digital Governance at THE NEW INSTITUTE. He is a serial entrepreneur in the legal, cybersecurity, and robotics sectors. Paul is a Fellow and Core Theme Leader for “managing information and technology in the public interest” at the Global Solutions Initiative. He is also a Distinguished Fellow at the Centre for International Governance Innovation and a Commissioner of the Global Commission for Internet Governance. Paul is the former CEO of ICANN, the global coordination body of the Internet. Paul was CEO of the Australian Government's National Office for the Information Economy and Deputy at the Australian Trade Commission. He was previously at McKinsey & Co. He is a member of the SAP Artificial Intelligence Ethics Advisory Panel. He holds a PhD from the University of Cambridge.

The authors wish to thank Jeffrey Arsenault, Professor Ian Brown, Maria Farrell, Tim Noonan, and Dr. Sherry Stephenson for their significant, substantive contributions to this paper. They are also indebted to Professor Andrew Briggs, Professor Laura DeNardis, Professor Kirsten Martin, Dr. Jonathan Fenton, Colm Kelly, Dr. John Klensin, Rebecca McKinnon, Scarlett McClure, Anouk Ruhaak and Blair Sheppard for extremely insightful comments.

The members of the Global Initiative for Digital Empowerment include:

- **Sait Akman** Senior Research Fellow, Centre for Multilateral Trade Studies at the Turkish Economic Policy Research Institute
- **Jeffrey Arsenault,** Cybersecurity Expert, TwistedLogic LLC
- **Stephen Balkam**, Founder & CEO, Family Online Safety Institute
- **Andrew Briggs**, Professor of Nanomaterials, University of Oxford
- **Michael Bruenig,** Dean, University of Queensland Business School
- **Joanna Bryson**, Professor of Ethics and Technology, Hertie School, Berlin
- **Anna Byhovskaya,** Senior policy advisor to the Trade Union Advisory Committee to the OECD
- **Laura DeNardis**, Professor in the School of Communication at American University in Washington, DC
- **Jane Drake-Brockman**, Institute for International Trade, University of Adelaide
- **George Ellis,** Professor of Applied Mathematics, University of Cape Town
- **Paul Grainger**, Director of the Centre for Post-14 Education and Work, Department of Education, Practice and Society, University College, London
- **Fen Hampson**, Chancellor's Professor Carleton University
- **Byron Holland**, President and CEO, Canadian Internet Registry Authority (CIRA)
- **Anne-Rachel Inne**, Senior VP Government Affairs Department, American Registry for Internet Numbers (ARIN)
- **Sye Munir Khasru**, Chairman, The Institute for Policy, Advocacy, and Governance (IPAG)
- **Beatriz Kira**, Senior Research and Policy Officer, Blavatnik School of Government at the University of Oxford
- **Hildegunn Kyvik Nordås,** Council on Economic Policies (CEP) and the Norwegian Institute of International Affairs
- **Peter Lewis**, Director, Centre for Responsible Technology
- **Ciaran Martin**, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government at the University of Oxford
- **Kirsten Martin**, William P. and Hazel B. White Center Professor of Technology Ethics and Professor of IT, Analytics, and Operations in the Mendoza College of Business at the University of Notre Dame
- **Russell A Mille**r, J.B. Stombeck Professor of Law, Washington and Lee University, comparative expert on US and German privacy and surveillance law
- **Desiree Miloshevic,** Special Advisor to the Chair of the Internet Governance Forum Multi-stakeholder Advisory Group
- **Tim Noonan**, Director, Campaigns and Communications Department, International Trade Union Confederation
- **Mike Orszag**, Head of Research, Willis Towers Watson
- **Andrés Ortega,** Senior Research Fellow, Elcano Royal Institute, Madrid
- **Alejandro Pisanty,** Professor of Chemistry, UNAM, Mexico; Former Director of ICANN, ISOC, and IGF
- **Julia Pomares**, Chief Advisor, Government of the City of Buenos Aires
- **Maria Fernanda Robayo**, Programmes Officer, Club de Madrid

GIDE

- **Rafal Rohozinski**, CEO SecDev
- **Güven Sak**, Managing Director of The Economic Policy Research Foundation of Turkey (TEPAV)
- **Patrick Sharry,** Fellow of the Australian Graduate School of Management
- **Dennis Snower,** Co-Director, Global Initiative for Digital Empowerment
- **Sherry Stephenson,** Convenor, PECC Services Network
- **Nick Thorne, CMG,** Former UK Ambassador to the UN
- **Bishop Paul Tighe,** Secretary, Pontifical Council for Culture, Holy See
- **Paul Twomey**, Co-Director, Global Initiative for Digital Empowerment
- **Heidi Tworek,** Associate Professor of History and Public Policy. University of British Columbia
- **Simonetta Vezzoso**, Department of Economics and Management, University of Trento
- **David Wilson**, Distinguished Professor of Biological Sciences and Anthropology at Binghamton University

Published by the Global Initiative for Digital Empowerment.

For publications enquiries, please contact info@thegide.org.

ISBN: 978-0-646-86668-0

GIDE

Contents

Executive summary

Although the digital revolution has unleashed a vast array of new opportunities for economic, social and political exchange, there is a misalignment of interests between the users and many suppliers of digital services. Building on unprecedented network effects, and consequent rewards to first movers (especially those who offer “free” services to maximise market penetration), many digital service providers have pursued a business model built on massive user surveillance and data aggregation. The largely surreptitious collection of vast amounts of information has fuelled a more than $515 billion market between data aggregators and entities seeking to influence their users.[1] But the billions of individuals whose data is collected are not part of this market, rather they are induced into a state of digital husbandry through the offer of “free” services. The misalignment between digital consumers and digital third-party funders is responsible for a wide variety of malfunctions, which ultimately threaten the continued functioning of our economic market systems; expose consumers, businesses and governments to widespread cybersecurity threats; expose users to far-ranging manipulation of attention, thought, feeling and behaviour; erode appreciation for objective notions of truth, undermine our democratic processes; weaken mental health; threaten fundamental human rights and degrade the cohesion of our societies. It also furthers international economic and social divides. As the United Nation’s Conference on Trade and Development notes, “In terms of economic development, it is important to ensure that developing countries are able to properly capture the value of the data extracted from their citizens and organizations.”[2]

These concerns have been broadly recognised for some years, and governments have sought to respond to protect their citizens mostly by evolving privacy rights through a consumer protection prism. But in taking a consumer protection approach, governments have failed to introduce market forces to the relationship between the individuals and the other two participants – digital service providers and the third-party influencers/funders. Further, the application of a “one size fits all” definition of personal data has failed both to keep up with how data collection has expanded and changed though technological change, and also to avoid

[1] Worldwide Digital Advertising in 2022, Statista: https://www.statista.com/outlook/dmo/digital-advertising/worldwide#global-comparison

[2] UNCTAD (2021), p. 65

unexpected consequences on the implementation of common goods aspects of the Internet's operation.[3]

Rather than just continuing to shoulder an onerous burden of trying to regularly update consumer protection/privacy regulation to keep up with technological and commercial changes among data aggregators and influencers, governments should move forcefully to gain the benefits of a properly functioning market through ensuring that citizens are active economic participants. Giving consumers the ability to control access, and on what terms, to their data, provides incentives throughout the value chain for economic resources to be allocated in their most productive uses in satisfying consumers' needs. Similarly, promoting such control gives individuals the ability to express social and political views and choices free from a non-transparent environment of implicit manipulation. This is the basis for true "digital citizenship," in two senses: first, empowering digital users to shape their digital networks in accordance with their own objectives and, second, enabling the economic markets to work in an effective and humane way in meeting digital users' objectives at minimum resource cost. Governments can move to achieve an active market role for citizens by:

- Adopting a multi-tiered definition for personal information with different policy requirements for each tier. We propose three types of personal data:

    - "Official Data" or **O-Data** is the sort of data normally required for entering a contract or satisfying government or major institution identity requirements. O-Data is to be controlled by the data subject but authenticated by trusted third parties. Building on the existing rules in Europe and elsewhere about the unique legal functions of data carried on identity cards or passports, we propose a new legal framework which makes this record the only way in which such data may be legally 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 – giving individuals control over who has access to their personal data and on what conditions. This power can be expressed by the data subjects though meaningful rights of association to give them access to collective representation to ensure effective market negotiations between individuals' interests and those of powerful data aggregators. Drawing on lessons from e-commerce, online banking etc., we urge giving individuals genuine control over their O-Data through easy-to-use technical tools and supporting institutions.
    - **P-Data** is "privy data" related to individuals, but which is not collective and does not require authentication by third parties. This data may be divided into "first-party data" (such as personal blogs and personal photographs) that are volunteered or generated by the data subject and observable by other parties, and "second-party data" generated by a second party about the data subject (such as location data from smartphones, records of a person's past purchases of goods and services) or inferred about the data subject from existing data (such as psychological data deduced from web searches). In this paper we refer to these two types as "first-party P-Data" and "second-party P-Data". The data subject is to be the only legal source of first-party P-Data. As per O-Data, individuals should be given genuine control over use of their first-party P-Data, through the above-mentioned negotiation of terms by skilled representatives, supported by

[3] For instance, the ongoing paralyzing debate about "WhoIs" data in the Domain Name System arising from definitions in the European General Data Protection Regulation. See https://www.eccia.eu/assets/activities/files/ECCIA_NIS2_paper.pdf

technical tools and supporting institutions.
Considering that second-party P-Data is not collected though any negotiation process with the data subject, such data should be used exclusively in the interests of the data subjects. The collection, purposes and consequences of use of second-party P-Data should be transparent to the data subjects.

- **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.[4] C-Data is subject to the same security requirements and restrictions on unpermitted onward transit as P-Data currently is under data protection laws. This data can encompass consumer associations, agricultural collectives, trade unions, financial collectives and much more. Some examples could include geographic data for digital maps, "smart city" data, aggregated data from banking and farming cooperatives, medical research data including that of under-served groups.
  We recommend that governments establish legal structure to support the establishment of "data commons" for C-Data. This includes ensuring that C-Data are under the control of effective, trustworthy, security-capable and competitive organisations that promote the benefits of data subjects and the broader society.

- Ensuring that long-standing rules in the offline economy to protect the vulnerable from manipulation by those holding intimate data on them (e.g. doctor-patient) apply to online actors as well. The offline test is that such data should be used in the best interests of the data subject. This test is not passed merely by a blanket assertion that the sharing of vast amounts of intimate data with unknown third parties provides more tailored advertising to the data subject.
- Applying the lessons from existing large-scale data management systems (such as the modern management of credit card transactions or the Internet's Domain Name System) to improve the cybersecurity around individuals' O-Data and reduce fraud to business, citizens and government.
- Ensuring that Artificial Intelligence actors adopt and promote these proposals, not only in the application of AI systems to personal data, but also in the collection and use of personal data in machine learning datasets which underpin the development of AI.

This paper also outlines in detail how such a policy framework could be put into practice through a set of implementation and audit models which are based on existing technical and business models of the Internet's Domain Name System and in e-commerce. These principles are "doable". There are also proposals to mitigate asymmetries of information and market power.

The benefits from the digital revolution are not immutably tied to the current personal data governance regimes. There exists no law of nature whereby the benefits from the new digital technologies can only be reaped through third-party finance of digital services to the users, combined with information-gathering and influence-projecting that lies largely beyond the consumers' informed consent. On the contrary, the benefits of the digital revolution are as little tied to the current digital governance regimes as the benefits of the industrial revolution were tied to the exploitative practices of many early factory owners. The central challenge of digital governance regimes lies in finding ways of making these regimes human-centred without sacrificing the technological benefits.

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

Finding the appropriate political “landing place” for these policy prescriptions is not immediately obvious. Apart from regional markets (such as the European Union which has been something of a governance first mover), there is a political failure in the sense that data flows don’t respect state sovereignty. But regulation is done by governments. That raises the question, what is the appropriate forum, or fora, to be addressing these issues? We intend to keep working as a Global Initiative to explore the best way for national governments and other stakeholders to work in concert in some kind of forum to address substantively these and similar digital governance issues.

Having recognised the international political challenge, economic history teaches that conditions in one country or region can result in an important transformation which is adopted more globally only over time. The industrial revolution emerged in Britain where the conditions were propitious – it did not rely on those conditions being instantly and globally available. Similarly, we consider that the political and economic structures and values in more democratic and open societies may well be best suited first to adopt the transforming principles we outline. The consequence should be a significant unleashing of innovation and wealth creation, as well as greater social equity.

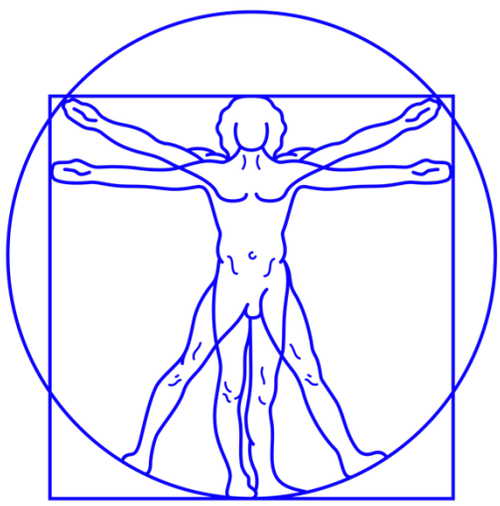
Our vision of the future is one in which:

- the opening up of access to and control of common data to the many will support a renewed flourishing of innovation;
- democratic accountability and control of the public entities that enforce the opening up of data for the common good, and the decision makers that determine what the common good is;
- 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 authorisation, 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;
- 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; and
- through establishing a properly functioning market (by ensuring that citizens are active economic participants), government consumer protection processes will not be the only forces to protect individuals in the face of ongoing technological and commercial changes among data aggregators and influencers.

Our human-centered approach

A key difference between the Global Initiative and other groups seeking to influence Digital Governance is our Unit of Measure.

Many take an institutional approach. We focus on the outcome on humans.



Many researchers and competition bodies take market participants as their main unit of attention. Other non- profits take the power relationship between nation states as their focus. Most economists focus on issues of inefficiency and inequality within a market framework. Even consumer organisations take the material benefits to consumers as their unit of analysis.

But our focus is on the human - not just consumers but also those who are still not users. And importantly we see humans as more than mere units of economic consumption and production. The last two centuries of capitalism have taught us that social solidarity, personal agency, environmental sustainability, as well as material gain, are each important, separate contributors to human flourishing.

1. Why we need human-centered digital governance

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

By contrast, the current digital governance regime is responsible for a wide variety of malfunctions, 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, erode appreciation for objective notions of truth, undermine our democratic processes, and degrade the cohesion of our societies.

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

In what follows, we will use the term "digital consumers" interchangeably with the terms "digital users" (the conventional Silicon Valley term), "digital customers" and "digital citizens". In particular, we will use the term "consumers" where it is appropriate to highlight the fact that people are consuming digital services and that these people are to be treated analogously to consumers in the offline world. We will use the term "digital citizens" to describe the goal of digital users becoming empowered to shape a digital governance system that enables them to achieve their individual and collective objectives. We also use the term "data subjects" to denote the people whom personal data is about; these people may not be consumers of digital services.

We also use the term "digital governance" to cover the laws, rules, contracts, terms and conditions, and norms which apply to the collection and use of data, particularly personal data, in the applications layer of the Internet. This is a more focused ambit than the commonly

accepted definition of the broader concept of "Internet governance".[5] We recognise that the operations coordinating the Internet's protocol layer and transit layer also utilise the data of digital consumers both for billing and other business purposes and for ensuring data reaches its intended destination. For business purposes we consider that their use of personal data falls under the principles of digital governance we propose below. But we do not consider that any personal data utilised solely for the purpose of technically ensuring that data reaches its intended destination, is automatically covered by the proposals below.

The aim of this paper is to consider the technological benefits from the digital revolution as separate from, though influenced by, the current digital governance regimes. Furthermore, we inquire how these regimes could be made human-centred (i.e., focused on the interests of the digital consumers) without sacrificing the technological benefits. In particular, we provide policy guidelines that would put digital consumers into the driver's seat, giving them ultimate control, individually and collectively, over their personal data and the economic, social and political influence to which they are subject.

The central flaw of digital governance: third-party funded digital barter

We begin with a simple question: In whose interests are digital personal data extracted, stored, manipulated and disseminated?

The question is analogous to the one concerning the interests that are meant to guide a competitive market economy. The answer to the latter question is the consumer. A competitive market economy, when it functions properly, is geared to satisfying the objectives of the consumers at minimum resource cost. The traditional explanation, repeated in countless economics textbooks, is that the ultimate purpose of all products is to satisfy the desires of the consumers, either directly (through consumption goods) or indirectly (through investment goods). The consumers pay for the products that they consume, and these expenditures drive all other economic activities. Under ideal conditions,[6] a competitive market economy allocates resources efficiently, so that it is impossible to make anyone better off without making others worse off. Such an economy cannot ensure equity (a fair distribution of resources across the population) and economists usually maintain that this is the responsibility of the government.

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

[5] In 2005, the Working Group on Internet Governance, meeting during the first phase of the World Summit on the Information Society, defined Internet governance as "the complementary development and application by governments, the private sector, civil society and the technical community, in their respective roles, of shared principles, norms, rules, decision-making procedures, and activities that shape the evolution and use of the Internet." See https://www.wgig.org/docs/WGIGREPORT.pdf

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

not well informed.[7] The choices that are open to the consumers are generally restricted by the digital service providers; they are not the choices that consumers would be given if the aim was to promote human agency for users in their individual and collective pursuits.[8]

Though digital consumers should be in ultimate control of the digital services they receive, the personal data they reveal and the influences to which they are subject, this does not happen. Rather, it is the third-party funders, working with the digital service providers, who ultimately drive the system.

Digital husbandry

It is important to distinguish the functioning of standard economic markets from that of digital markets. In standard economic markets, producers sell products to consumers and receive revenue in return. This trade is "visible," in the sense that it counted in the national income and product accounts.

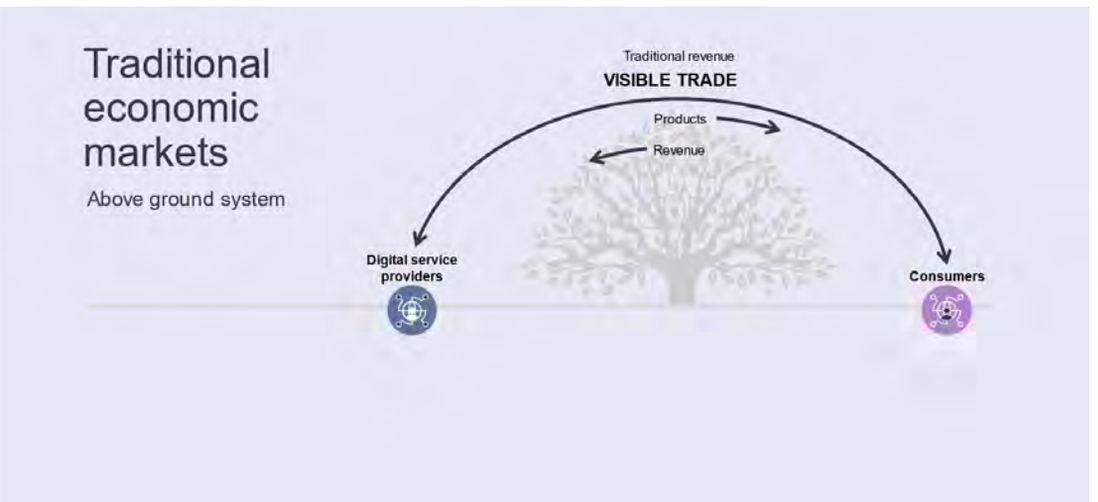


Figure 1: Standard Economic Markets

Under the current digital regimes, 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 them. In other words, *the current regimes are characterised by "digital barter" that is both "information-gathering" and "influence-bearing".*

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

[8] 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 organisation 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. Since user consent is usually not well-informed, 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.

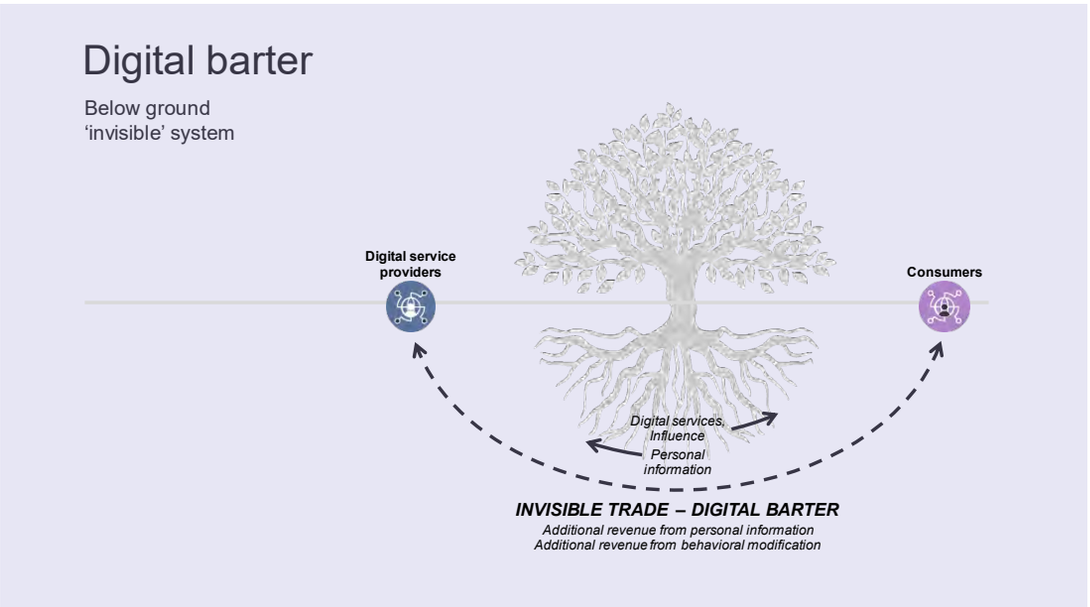


Figure 2: Digital Barter

This digital barter is financed by "third-party funders," who are influencers, comprising both traditional producers (who aim to influence the digital consumers through advertising) and other influence-wielding parties (who aim to influence the political and social behaviour of the digital consumers). In short, the third-party funders 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.

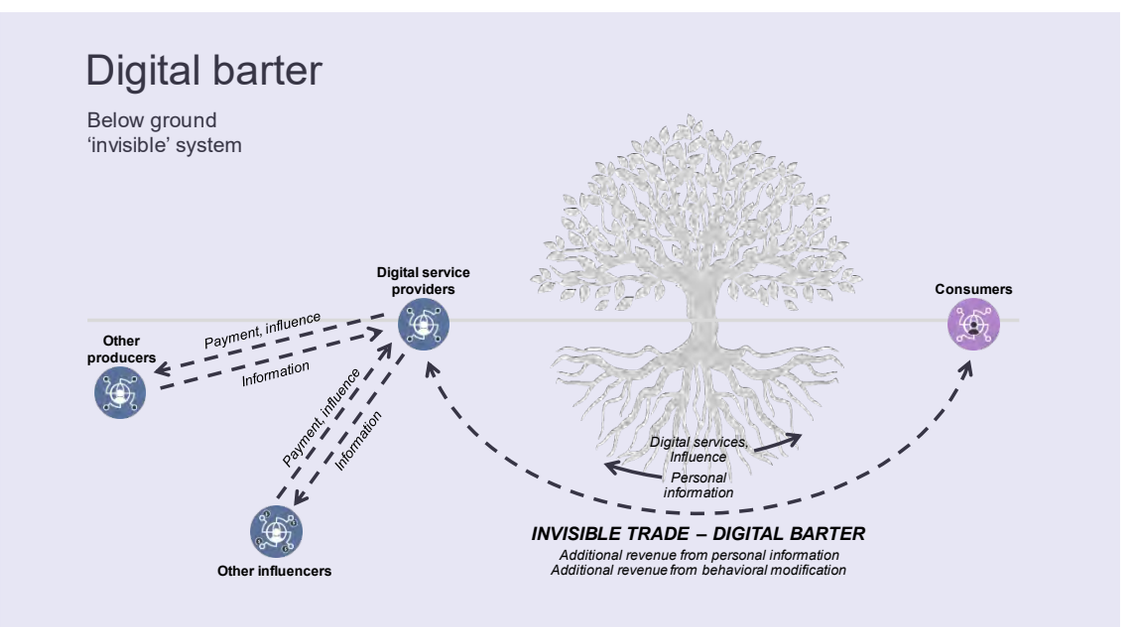


Figure 3: The Cross-Subsidisation System

Whereas the standard economic transactions are all visible (measured and counted in GDP), the digital barter transactions 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 digitisation proliferates, the visible trade is being shaped increasingly by a growing digital "shadow domain" lying outside markets and often outside our perception and understanding.

It is apparent that this is an elaborate system of cross-subsidisation. 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 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 modification of economic behaviour (allowing them to mould the consumers' preferences towards their profit-making products). The other influence-wielding parties receive their payoffs in kind, through modification of political and social behaviour (such as that affecting election results).

In short, it is the interests of the third-party funders that drive the digital system. Their control is based around large quantities of personal data, much of it collected by data brokers with whom the consumer has no contractual or other relationship, which may be used to manipulate digital consumers' preferences to influence purchasing, voting, and many other behaviours (Zuboff, 2019). The third-party interests are ultimately responsible for the digital services that the consumers receive, the personal information that the consumers reveal about themselves, and the ways in which consumers' choices are manipulated.

The digital service providers seek personal data about consumers and influence their choices in order to generate advertising revenues or proceeds from the sale of political or social influence. The third-party funders pay for the digital services in order to extract information about the consumers and thereby target their third-party influence more effectively and individually. When the influence takes the form of advertising products, it leads to revenues from these products. When the influence is political and social, it leads to outcomes that state or non-state agents find worth pursuing.

In short, the digital consumers are being used by the third-party funders. This phenomenon has been called "digital serfdom" (for example, Fairfield, 2017). Like serfs, digital consumers receive something of value in return for services of value to their handlers. This is an exchange in kind; it does not involve pricing in economic markets. Like serfs, digital consumers are at a great disadvantage in the balance of power and information. This digital governance system, like serfdom, is profoundly inequitable and inefficient.

This market failure is not limited to developing economies. As the United Nations Conference on Trade and Development (UNCTAD) notes on global personal data, "there are not properly developed and formalised raw data markets… There is no marketplace with supply and demand for raw data; they are currently basically extracted from users."[9]

The interests of the third-party funders are not well aligned with the interests of the users. In this sense, the current digital governance system is not human-centred. It does not place ultimate value on the agency of the human beings using the digital services. It is not designed to promote the fundamental needs and purposes of these humans, as individuals and as social creatures. It is not inherently concerned with the promotion of human freedom, empowerment and social belonging.

[9] UNCTAD (2021), p. 18

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 (see, for example, Bogust, 2007; Fogg, 2002; Moon, 2000; Reeves & Nass, 1996).

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 (see, for example, Oinas-Kukkonen & Harjumaa, 2008). 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. Apart from slavery, this is the first time in human history when people cannot shape their social relations in accordance with their own interests, but rather are constrained to connect with one another through prefabricated channels of communication that ultimately serve the objectives of the third-party funders.
- *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. Hence digital network providers are incentivised to deploy algorithms which reinforce social conflict.
- *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.
- *Persuasion*: Digital network providers' aim to earn revenue from advertising and other persuasive activities, which 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.

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.[10] Furthermore, the system also gives digital service providers inadequate incentives to protect their users'

[10] See UNCTAD (2021) Chapters 3 and 4, and UNCTAD (2019)

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

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

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

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

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

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

These asymmetries also lead the digital service providers to give consumers limited choices, such as the choice between remaining connected to their economic and social world and giving up control over their personal information. These limited choices are responsible for the widespread sense of disempowerment, arising from attention capture, manipulation of preferences, and misleading information.

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

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

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

In short, policy makers have focused more on treating the symptoms of the digital governance dysfunction rather than tackling the underlying disease, namely, third-party funded digital barter and the resulting disempowerment of digital consumers. This policy deficiency helps explain why the many efforts, over the past two decades, to make the digital regime more transparent, more equitable and less exploitative have met with such limited success.

A review of recent international regulatory efforts to address the sort of problems identified above, shows an emphasis on either company-on-company power structures (e.g. competition policy) or consumer protection initiatives (including privacy) by governments. It does not uncover efforts to address the structural empowerment of consumers within the overall market.

A noted recent example of the consumer protection model is the European Union's draft Digital Services Act (DSA). It proposes a "notice and action" mechanism for the removal of illegal products, services or content by online platforms, such as social media and marketplaces. Very large online platforms (VLOPs) will also be required to review, amend and be audited to address risks they pose regarding the dissemination of both illegal and harmful content, the spread of disinformation, and their algorithms to recommend what users see.

In January 2022, the European Parliament introduced key changes mostly limiting profiling-based advertising by VLOPs: banning their application to minors and prohibiting targeting individuals on the basis of special categories of data which allow for targeting vulnerable groups (e.g. on the basis of race, political opinions, religious beliefs, trade union membership, biometric data, health data, or sexual orientation). Further, online platforms should be prohibited from using deceptive or nudging techniques to influence users' behaviour; indeed, they should be required to be more transparent about consumer choices, including information on how their data will be monetised.

As it now stands, the draft of the DSA is a significant step to help alleviate some of the negative symptoms in the present digital governance. But it does not cover the full swathe of the economy (all companies, global markets, IoT, Artificial Intelligence etc.), and does not provide individuals with full transparency and control as to who has information on them. (Indeed, amendments at the European Parliament seeking to limit collection of data beyond the present limits of the GDPR were not successful.) Furthermore, it does not establish the long-term benefits of fully integrating consumers as full economic actors in the digital data market.

Like other policy efforts on digital governance, this policy initiative is analogous to restricting the latitude of the serf masters. It does not amount to the abolition of serfdom.

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

Since the fundamental flaw of the current digital governance regime is the lack of alignment between the interests of the consumers and the interests of the third-party funders and the digital service providers, policies that address the symptoms of this underlying flaw are likely to be ineffective in combatting the inherent injustices and inefficiencies of the current system. For example, protecting privacy by requiring users to agree to the terms and conditions of digital services cannot ensure informed consent, because these terms and conditions are generally too cumbersome and opaque for most consumers to read and understand, particularly in the context of complex nested agreements among digital service providers, Internet service

providers and third-party funders. Furthermore, even if consumers were able to digest all the terms and conditions of their digital services, there would be no assurance that consumers were allowed to choose from a portfolio of options allowing them to satisfy their needs most efficiently.

Adverse implications of the current digital governance regime

The adverse implications of the current digital regime are many and grave. In what follows, we provide an overview of the most important deficiencies: the current regime systematically creates economic inefficiencies; it provides systematically inadequate protection of privacy and inadequate cybersecurity; it generates large economic, social and political inequities; it systematically exploits users' psychological weaknesses and makes them vulnerable to political, social and economic manipulation; it disempowers the digital users; and it threatens a range of fundamental human rights. Thereby, the current regime undermines the functioning of economic markets, democratic processes and social cohesion. Let us consider each of these deficiencies in turn.

Inefficiencies

The system of third-party digital barter is massively inefficient, for a variety of reasons. First, the market economy becomes inefficient because the prices of the digital services do not directly reflect the value of these services to the users. Needless to say, the prices of digital services cannot do so, since so many digital services are free and many of the rest are grossly under-priced (in order to induce the digital consumers to reveal information about themselves, which can be used to influence their offline behaviour). Consequently, it is 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 the third parties to whom the data may be resold. This asymmetry of information is inefficient, since the exploitation of informational advantages by the digital service providers and data aggregators is wasteful, because these decision makers do not have to take full account of the users' interests. This asymmetry of information greatly reinforces the asymmetry of market power between data subjects and digital service providers, another source of inefficiency addressed below.

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

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

experience of data breaches, and excessive discounting of future costs relative to immediate benefits. The digital service providers and data aggregators exploit these cognitive biases with a view to the benefits accruing to themselves, but not the associated costs to the digital users.

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 recognise probabilistic or uncertain harm.

These inefficiencies are tolerated by the data aggregators and digital service providers, since what they lose from these inefficiencies, they make up handsomely through the market power gained through the current digital governance regime. Hal Varian, the chief economist at Google, argues that data nowadays are plentiful and thus virtually worthless, whereas the designers of the networks are scarce and thus generate most of the value of the digital network services.[12] This argument is self-serving. It is impossible to assess the marginal contributions of data users and network designers when one of these groups works for free. Furthermore, as Posner and Weyl (2018) note, it is far from clear that the marginal value of the data generated by network users declines with the amount of data, given that the data are used to handle more and more complex problems (such as face and emotion recognition and predictable cognitive processes).

One could argue analogously that just as the value of one consumer's personal data is negligibly small in comparison to the value of the aggregated digital services, so the value of one employee's work is negligible in a global supply chain. By this line of reasoning, most of the value comes from combining the work of countless employees working in a variety of countries to produce the commodities generated by the global supply chain. But this reasoning does not stop the employers from paying wages to their employees.

In short, by encouraging "third party-financed digital barter," the current digital governance 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 or severely curtailed.

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 maximise the returns of the digital service providers or not participating in the modern information society.

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

Data authenticity

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 can be 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, duplicity and criminality.

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 emphasise the benefits of data sharing, due to improvements in the allocation of resources and in the rate of innovation (for example, Varian, 2009; Veldkamp et al., 2019; Veldkamp, 2019). Some analyses recognise the importance of privacy concerns, but commonly claim that data markets are able to balance privacy concerns (for example, Posner, 1981; Stigler, 1980; Varian, 2009) against gains from data sharing (for example, Laudon, 1996; Posner & Weyl, 2018). 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 (for example, Ibarra et al., 2018; Posner & Weyl, 2018).

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 underutilisation 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 characterised as surveillance systems, used particularly by digital service providers to target advertising individually to users. The 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 mostly 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.[13] In some cases, users have the possibility of opting out of some surveillance, but often in return for significant loss of service.[14]

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 government directives and regulation) 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 cyber vulnerabilities through digital governance is of great importance.

Incidents of online fraud continue to grow. With the expansion of digitisation and online financial services, cybercriminals have been able to exploit computer systems vulnerabilities and the lack of an authoritative digital identity system to expand digital identity fraud. For instance, the UK fraud prevention service Cifas reported that cases of digital identity fraud increased by nearly a third in the five years up to the end of 2019.[15] The financial cost to consumers and businesses is massive. One report suggests that from 2020 to 2024 such fraud stole more than $200 billion just from the e-commerce, banking and money transfer, and airline sectors.[16]

Phishing, spoofing, identity theft and social engineering result in millions of account takeovers and the theft, extortion, or re-purposing of assets. In addition to improved human and technological responses to these attack vectors, the proposals in this report can substantially help reduce the threat by providing authenticated personal identity data held securely and accessed by businesses only through a cryptographically specific transaction.

Inequities

The current regime creates major accretions of market power in the hands of the digital service providers, as there 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.

---

[13] 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."

[14] 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.

[15] See https://www.fraudscape.co.uk/#welcome

[16] See https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report

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 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.

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 maximise 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 (see, for example, Baumeister et al., 2001). 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.

Third, since digital service providers seek to maximise 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 that require sustained effort. Users are encouraged to multitask, but the human brain does not multitask in the sense that we understand multitasking in our daily lives; instead, it switches rapidly between different activities. This stressful alternation is supported by adrenaline and cortisol, which over the long run makes it difficult for us to be tranquil and content; and it also has an inflammatory influence on our brain cells, which may be linked to depression.[17]

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

[17] Bullmore (2018) examines the link between inflammation and depression.

protracted distraction and interruption hurts our cognitive faculties, hurts our intelligence (see Gazzaley & Rosen, 2016), and harms our productivity.[18]

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 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 that currently control the media content have a natural tendency to err on the side of encouraging user attention, which is often associated with aggressive behaviour.

Finally, the digital intermediation of much interpersonal communication through social media tends to promote shallower interpersonal relationships, both because direct interpersonal interactions are frequently interrupted through digital exchanges and because the large amounts of time we spend on social media come at the expense of direct interactions. Our concern with being "liked" on social media leads many to spend time accumulating large numbers of social media "friends" rather than cultivating unmediated personal relationships through sustained interactions in the physical world. Our emotional life, as a result, becomes shallower (see Carr, 2010).

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. The ultimate economic and political objectives that drive this manipulation are those of the third parties who fund the digital barter.[19]

It is important to emphasise 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 users have consented, and no independent audits associated with graduated penalties for misconduct.

Vulnerability to social manipulation

The revenues from advertising and other interest-selling depend on user attention. As noted, 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. In this way, the current regime undermines 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 organisations, educational communities, political movements, and many other social groups. Of particular importance in this regard are the "gatekeeper platforms" that connect the influence of buyers (in the economic, social and

[18] Puranik et al. (2019) examines the effects on productivity.

[19] 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.

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.[20] 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.

Vulnerability to economic manipulation

The content and organisation of information that reaches the users is shaped by the objectives of the third-party funders. Since the content and organisation 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 – including the exploitation of behavioural biases and transaction costs, as well as the generation of massive asymmetries of market power – are built.

What empowerment does an individual have in the digital economy when she or he is the product that is being transacted? In 2020, the value of online advertising in Europe was €69 billion.[21] This is the value of having 500 million Europeans' personal data aggregated to promote the marketing of goods and services. And yet digital consumers had no mechanism to specify the terms on which they wanted their data to be accessed. There is presently no mechanism for people to actually negotiate their way into the market. It reminds us of the early days of the industrial revolution, where workers came into factories, but had very few rights to negotiate their conditions and their pay.

Disempowerment

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. This powerlessness arises from an awareness that one needs to be digitally connected nowadays in order to be functional in the advanced and emerging nations. But the digital connections come prearranged and prefabricated by digital service providers, in accordance with third-party interests.

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 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

[20] For instance, the Google platform supports Google Search, Google Home digital assistant, Google Pixel smartphone, Gmail, Google Meet, Google Translate, Google Calendar, Google Earth, Google Maps, Google Play, YouTube, etc.

[21] See https://iabeurope.eu/all-news/iab-europes-adex-benchmark-2020-study-reveals-european-digital-advertising-market-achieved-positive-growth-in-2020/

most significant social affiliations in the offline world – affiliations driven by deep personal relationships with people we respect, trust and care for – our social networks are shaped significantly by the objectives of the digital service providers to capture the attention of their users as long as possible, to attract more users, and generate advertising revenue.

The resulting sense of disempowerment is compounded massively by the Internet of Things (IOT), whereby material objects communicate with one another, largely outside the awareness of people. These cyber-physical communications have turned the Internet into a control system in the hands of those who manage the cyber-physical information flow.[22] In practice, people's ownership of objects is 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.

Threats to fundamental human rights

On account of the deficiencies above, the current digital regime is systematically prone to threaten fundamental human rights, for example, 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;
- **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 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 untransparent use of data through the third-party funders of the digital networks; and
- **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 labour markets of the gig economy.

Giving users control

Since influencers in the form of third-party funders drive the digital service system and since the objectives of the influencers are not aligned with the users' authentic needs and purposes, economic prosperity (measured in terms of the goods and services produced by the influencers) has become decoupled from social prosperity (measured in terms of the wellbeing of the digital users). The digital 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.

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

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 (i) giving individuals the right to grant or withhold personal information in accordance with their individual objectives, within the existing legal, political and social constraints, (ii) 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, and (iii) creating governance systems that prevent large asymmetries of information and power. Thereby, digital users can gain the agency required for true "digital citizenship".

People thus 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, reinforcing liberty and democratic values and generating knowledge and innovation at unprecedented scales – now needs to be embedded 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.

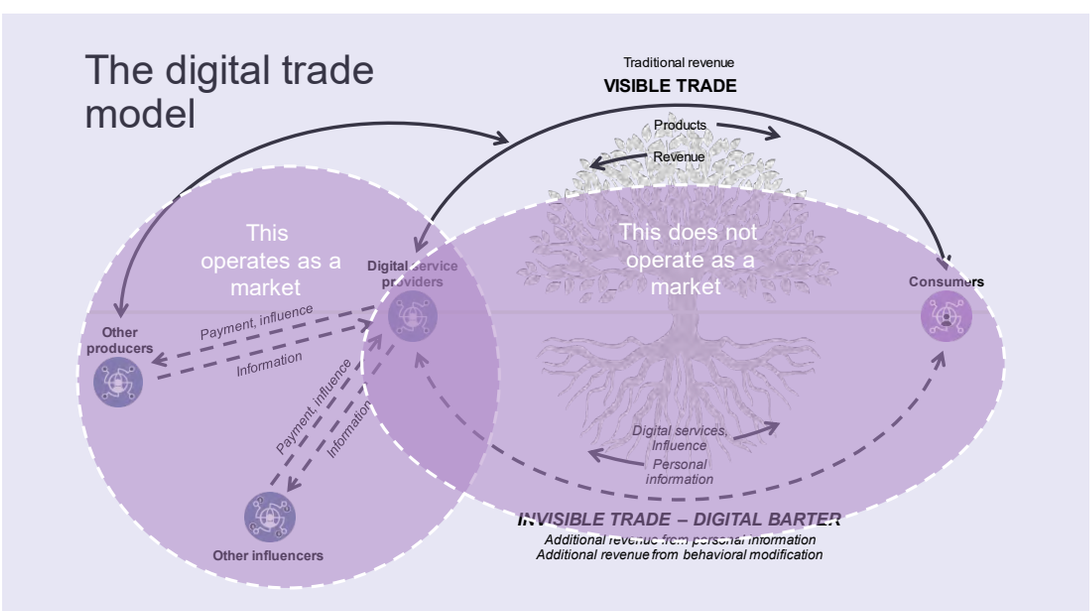


Figure 4: Towards Recoupling Economic and Social Prosperity

In the left-hand side of the diagram, the producers engage in digital trade with the digital service providers, buying and selling digital services and personal information. These transactions may involve compensation in money or in kind. The upper part of the diagram depicts the non-digital trade, in which products and information are traded in return for revenue, and in the lower part of the diagram, digital trade is depicted in analogous terms, again either monetary or in kind. Thereby the "shadow domain" of the current digital regime (comprising non-market, largely non-conscious activities of a duplicitous system) have been eliminated.

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 rationalised 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.

Putting the human into digital governance

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

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

Putting humanism at the centre of digital governance involves taking seriously the fundamental human needs and purposes of human beings. It means constructing a digital governance system that recognises the dignity of the person and recognises that humans are both individuals who require freedom and social creatures who derive life meaning in conducting personal relationships and belonging to social groups, both of their own choosing.

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

Currently these problems are addressed largely in isolation from one another, for example, through competition law, privacy law, intellectual property legislation, consumer protection legislation, commercial law, and more. We argue, however, that since these problems may all be understood as symptoms of a common cause – the lack of users' control, individually and collectively, of the data about themselves – the existing policies could be powerfully supplemented through human-centred digital governance.

To this end, we propose four broad policy guidelines, each of which serve the purpose of moving control over personal data from the third-party funders and digital service providers to the users of digital services. There is much that we can learn in the online world from the ways in which these principles were pursued in the offline world.

The thrust of this movement is to be understood historically as analogous to the gradual shift of economic power in the early stages of capitalism, from monarchs and feudal lords to small-scale entrepreneurs, who made their living by responding to their consumers' demands. Afterwards, the shift of power from domineering industrialists toward a more balanced relationship between employers, employees and customers from the middle of the 19th century to the middle of the 20th century in the advanced industrialised countries was an important factor in the spread of the "mixed economy" (containing free enterprise, supplemented by government finance and provision of education, health, social security and other areas) after World War II. These experiences served human needs and purposes. Human-centred digital governance may prove to be successful in the digital realm for the same reasons.

In broad outline, the world may currently be divided into four governance regimes: (i) the American regime, in which a small number of digital service providers enjoy preponderant market power and digital information advantages, (ii) the Chinese regime, in which the state enjoys preponderant informational advantages, supported by a small number of digital service providers, (iii) the European regime, in which digital service providers are far less powerful and the state's regulatory power focuses on protecting the rights of digital users, (iv) the rest of the digital world, with little market power and little regulatory power, but a strong drive to narrow the digital divide. Due to the inherent popularity of governance regimes that promote individual and collective empowerment, the option of human-centred digital governance is relevant for all of these regimes. But there is no reason to believe that human-centred digital governance is likely to be adopted in the same form across all four regimes, much as the mixed economy has not been adopted in the same form across countries.

In the offline world, free market economies coexist with social market economies, state-guided capitalist economies, and more.[23] These economic systems are thoroughly integrated in global value chains, trading goods and services and moving financial and physical capital. Along analogous lines, different digital governance regimes may be expected to connect with one another through the exchange of information in accordance with mutually agreed terms. Human-centred digital principles may be relevant to these regimes in the same way as the principles of voluntary exchange have been relevant to the diverse mixed economies. In much of the offline world, feudalism, slavery, indentured servitude, child labour and other institutionally exploitative practices have gradually been replaced by more human-centred ones, despite the institutional and cultural diversity. The same may be expected in the digital realm, but in fast motion.

At present, the EU digital governance regime is most closely aligned with the human-centred principles advocated here. In fact, our proposed policy guidelines are already compatible with the EU's General Data Protection Regulation (GDPR), the Digital Services Act package[24] (encompassing the Digital Services Act (DSA) and Digital Markets Act (DMA)) and other EU digital directives and acts. As such, they can be understood as a simplification and development of existing legislation.

---

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

[24] https://ec.europa.eu/digital-single-market/en/digital-services-act-package

The proposals below encompass and integrate into one coherent framework the digital policy measures extending across a wide variety of policy domains, including consumer protection, innovation, digital trade, competition, taxation, privacy, cybersecurity, collective representation, data commons, and human rights. Our proposals also cover a range of additional important issues, including digital citizenship, business ecosystems to support private and collective data, and combating misinformation and hate speech.

Such has been the lure of human-centred governance systems in the past, that we have reason to expect a similar attraction to digital governance regimes in the future. We claim that the more economic areas such as the EU or the Americas adhere to the policy guidelines articulated here, the more economic activity – both digital services and the associated non-digital goods and services – will be attracted to these areas. On this account, human-centred digital governance may become an important influence on digital regimes elsewhere as well.

2. How can we build a human-centred digital governance?

Appropriate goals for government policy

All the deficiencies above have received significant public attention and need to be addressed by setting appropriate goals for government policy.

The inefficiencies from third-party funded digital barter are associated with a loss of productive capacity and living standards (relative to efficiently traded digital services). The accretions of market power generate inequities arising from vast inequalities of income, wealth, skills and employment opportunities. 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 unravelling of social cohesion in many countries.

Conventional economic analysis, by focusing on the allocation and distribution of goods and services, hides many of the most serious problems of the current digital governance regimes. The above-mentioned deficiencies often undermine personal empowerment and social solidarity. For example, to understand the need for privacy and protection from manipulation, it is important to recognise 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 recognise 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.

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 & Katz, 2006).

While these considerations are important, they 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.

In short, a full understanding of the deficiencies of the current digital governance regimes requires recognition that solidarity and agency are human needs that are as basic as the need for consumption goods and services. As the success of the human species rests largely on cooperation, innovation and niche construction (the process by which an organism shapes its own environment), we have inherited the need to socialise (particularly in groups of limited size) and the need to use our capacities to shape our environment (see, for example, Henrich, 2017).[25] These needs for solidarity and agency, alongside the need for consumption, are present in all cultures.

These fundamental 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).[26] 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 (see, for example, Atkinson & Feather, 1966; Pang, 2010) and status-seeking (seeking social standing and social influence)[27] and self-interested wants.[28] 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 digital governance regimes can all be understood as obstacles to the satisfaction of these fundamental needs and purposes. By thwarting our capacities for social cooperation and agency and by introducing inefficiencies into the market system, these regimes make it more difficult for people to cooperate with future generations by ensuring environmental sustainability. Solidarity, agency, material gain and environmental sustainability are each important, separate contributors to human flourishing. [29] 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.

A reform of the digital governance regimes should aim to promote people's communities (solidarity to their social commons), their sense of empowerment (agency to influence their fate through 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). Our classification scheme, policy proposals and implementation options, described below, are meant to serve these goals.

[25] While online platforms have given users innovative ways to socialise, 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.

[26] 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).

[27] This motive is analysed, for example, in H. Heckhausen (1989) and J. Heckhausen (2000).

[28] This motive is covered by the individualistic preferences of neoclassical utility theory in economics.

[29] These objectives – Solidarity (S), Agency (A), material Gain (G) and Environmental sustainability (E) – are measured over a large number of countries and extended time periods by SAGE dashboard of Lima de Miranda and Snower (2020).

Linking goals to practical policy and implementation

The central claim of this paper is that the benefits of the current digital regime can be retained, while the above-mentioned problems 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 four 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 models* for these policy proposals that enable data subjects to gain appropriate control over, and use of, 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[30];
- 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 authorisation, 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;
- online influence 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[31];
- 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,

[30] Note that The European Data Act seeks to create a mechanism for private company data to be used in the public interest.
[31] The European Data Act gives users full rights over the data generated by their own connected products.

along with related European regulations and laws[32] can be complemented 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.

To address these above-mentioned deficiencies, we present our new classification system for personal data, which permits our policy proposals to be readily understood, followed by the proposals themselves and guidelines for their implementation.

Classification: Three realms of personal data

We distinguish between three types of personal data:

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

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

C-Data is "collective data," which data subjects agree to share within a well-defined group or community of interest for well-defined collective purposes. This data may be shared through voluntary agreements or through democratic processes established through law.[33] It is important that there is an open and accountable process for defining these processes and checks and balances to ensure that the collective purposes cannot result in harm to individuals especially the vulnerable and less empowered (e.g., children, minority groups, migrants, the sick, the homeless). C-Data is subject to the same security requirements and restrictions on unpermitted onward transit as P-Data currently is under data protection laws. This data can encompass consumer associations, agricultural collectives, trade unions, financial collectives and much more. Some examples could include geographic data for digital maps, "smart city" data, aggregated data from banking and farming cooperatives, medical research data including that of under-served groups.

On this basis, we propose the following four sets of policy proposals.[34]

[32] 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

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

[34] The practical implementation of these proposals is to be contained in a further paper.

3. Policy proposals

Proposal 1: Control over O-Data

Proposal 1a: O-Data must receive official (Generally Trusted Source) authentication, and this is to be the only legal source of this data.

Proposal 1b: Give individuals genuine control over use of their O-Data through easy-to-use technical tools and supporting institutions.

In other words, O-Data is to be controlled by the data subject, but authenticated by trusted third parties, under a new legal framework which makes this record the only way in which such data may be drawn by third parties.

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. [35]

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

[35] 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.

The content of O-Data requires authentication by legitimate sources, but data subjects are to control and manage its use.

Providing direct, effective control of consumers' O-Data and first-party P-Data calls for mainstream use of both existing and 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."[36] As discussed below, the Australian Consumer Data Right regime has already commenced down this path.

Currently there are few if any laws requiring that all parties must access official data in a uniform way from an authenticated user-controlled source. The appropriate offline 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. Similarly, in most cases a passport is required to cross a border. The data on the passport could be sourced by the receiving immigration officers from any other source, but to ensure the integrity of the broader system, the law requires it be sourced only from an authoritatively issued passport. 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.[37] Whenever a company or other party requires this data, it should not be inferred or observed, but be drawn from the user-controlled authoritative source.[38]

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.[39]

This mechanism allows the individual to say to the data aggregator "I don't care if you can pull all my O-Data together from other sources, you can only use the O-Data you require if you retrieve this authenticated data from this source which I control and which you can only access

---

[36] 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.

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

[38] This requirement is similar to the authoritative root system for a limited set of data which drives the Domain Name System. This is an adaptable technological model for which the technical architecture can be developed in a straightforward manner. Just as the authoritative data fields in a DNS record are prescribed (open to ongoing standards review and change), 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.

[39] 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 to the individual in dealing with global platforms and others.

on the terms I approve." Then the citizen can individually, or more likely as part of a collective, negotiate the terms.

Once the citizen has representatives who can negotiate on her behalf, the skills in the online data market will begin to shift. Experts with deep understanding of the online market in personal data will not just be employed by the data aggregators and the advertisers. Some of the skills of that market will move to the consumer side. Then we may experience more of a market, rather than digital husbandry, where consumers are able to get more agency and value out of any decisions they make to allow others to interact with their own personal O-Data, and consequently, first party P-Data. This is a prerequisite for empowering digital citizenship.

Proposal 2: Control over P-Data

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

This proposal is analogous to Proposal 1a

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

Providing direct, effective control of first-party P-Data calls for mainstream use of new technological and institutional mechanisms for managing personal data, whereby the control of this data is handed from the digital service providers to the data subjects. The implementation of the users' right to directly manage and control of their first-party P-Data will build on the system established above for O-Data. First-party P-Data (photos, geo-location data, etc.) are 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 use and financial terms for first-party P-Data as part of the right for accessing the authoritative 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 laws requiring that P-Data be held and used in the interests of the data subject.

Proposal 2c: Use second-party P-Data always 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).[40]

By implication, data that is inferred about the data subject is also to be used always in the interests of the data subject. For this purpose, the data subject needs to have automatic access to the data inferred about him- or herself and to determine what data is to be held by the second party. The inferred data must be transparent and clear, i.e., understood by the data subject in a limited time frame. The terms and conditions that a second party sets for digital services tied to inferred data must be proportionate to the agreed purpose of the data collection. Any actor who

[40] 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 travellers at border controls, this data may belong to the data commons, as specified by existing laws.

collects personal data about an individual should be required to act on, share, or sell this data only if it is consistent with that individual's interests. Data brokers who hold intimate knowledge of individuals need to be held to a fiduciary-like standard of care for how their data may be used (Balkin, 2016). This would make data brokers responsible for how their products and services were used to possibly undermine individual interests.

Establishing 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 propose that the test be grounded in existing human rights law. With reference to Europe, we would suggest 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.[41]

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, is 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. Legal protections can be drawn from "fiduciary law" frameworks, which consider the expertise, benefits and confidences in trusted, but informationally imbalanced professional relationships (Balkin, 2016).

There is a profound, yet relatively easy to implement, step to create such a fiduciary duty for data brokers. Governments should extend the regulatory requirements they have for doctors, 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. Any actor who collects or uses intimate data about an individual should be audited to ensure they act within a defined duty of loyalty. This would force alignment of the interests of the target/consumer/user and the firm in the position to manipulate. When data brokers holding intimate knowledge of individuals are held to a fiduciary-like standard of care for how their data may be used, the data brokers become responsible for how their products and services were used to possibly undermine individual interests.

An additional step would be to ensure digital service providers only sell access to consumer information to second parties – whether by selling the P-Data or by selling access to the consumer through tracking technology on their app or website – who are audited to ensure they abide by a duty of loyalty to the consumer. This would put the burden to understand the actions of second parties to track and target consumers on the consumer of digital services. Since the digital service providers are the actors who collect money from the second parties, selling access to consumers and their data, these providers should be willing to conduct due diligence to ensure the second parties will act in their consumers' best interest (abide by a duty of loyalty).

[41] 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

Proposal 2d: The collection, purposes and consequences of use of second-party P-Data should be transparent to the data subjects.

Transparency and accountability in the use of second-party P-Data and C-Data online should be analogous to that used offline. Manipulation works because the tactic is hidden from the target. The governance goal is to make the basis of manipulation visible to the target and others, i.e., make the type of intimate knowledge used in targeting obvious and public. This might mean a notice (e.g., "this ad was placed because the ad network believes you are diabetic") or a registry, during hypertargeting, to allow others to analyse how and why individuals are being targeted.[42] 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, and what the diagnosis is. They are entitled to a second opinion on the data. In other areas, where a lawyer, realtor or financial advisor has intimate knowledge and could profit in a way that is detrimental to their clients, they must disclose their conflict and the basis for their conflict. Transparency and accountability online and offline could be brought into consonance with each other.

Proposal 3: Control over C-Data

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

A data commons is a legal entity that protects and uses the data of members to serve defined collective objectives, subject to a fiduciary duty to serve their interests.[43] 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 commons. 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.

The data commons is a defined and protected structure to which people can delegate the stewardship of certain subsets of their P- and O-Data. It may allow other organisations – for example, public bodies, companies, researchers – access to the data, subject to the preferences of the data subjects and in line with policies set collectively and always in their

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

[43] 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).

interests. The members collectively set the terms for how their data is shared and direct where the benefits created should go. Execution of these objectives is delegated to the data commons trustees who must ensure the commons carries out its fiduciary obligations to the data subjects.

Also key to ensuring both the conduct of the commons and the overall competitiveness of the data environment is that people's data is portable and practically interoperable. People can withdraw their data and decide not to share it, find an alternative or even create a new data commons to further their collective interests and goals.

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

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

The current system limits the willingness of citizens to share all forms of their own data, particularly health data, to secure collective goals, because of the potential individual cost and risk to them in an untrustworthy data environment. In some cases, C-Data collected by third parties may even be used to secure anti-competitive advantages against the data subjects, as for example with regard to farm and cooperative-level agricultural productivity data.[44] Large-scale datasets about the public – such as smart city data – should be evaluated to assess whether both their value and the risk of misuse merit these data-sets being managed in data trusts or commons, despite a clear fiduciary obligation to the data subjects.

Legislative support is required to create minimum legal definitions, protections and obligations for a range of data commons to be created. Drawing on existing types of organisations including clubs, cooperatives, trade unions and trade associations, legal guidance and definitions will encourage the emergence of data commons that identify and meet currently unmet demand for data sharing that protects and extends the interests of data subjects. Legislation may also be needed to ensure data commons identify and carry out the data-sharing policies of subjects and ensure appropriate privacy and security standards are met. The underlying guidelines for management of data trusts as a commons can be derived from Elinor Ostrom's Core Design Principles on the management of common pool resources (see, for example, Ostrom, 1990, 2010a, b; Wilson, Ostrom & Cox, 2013).

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

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

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

Proposal 4: Address digital power asymmetries

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

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

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

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

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

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

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

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

In the product market, consumers' rights are supported through consumer protection legislation. Protection against discrimination based on protected characteristics (such as gender, disability and age) is supported through equality and human rights agencies (e.g. the EU Fundamental Rights Agency). Digital users who are vulnerable to economic, political or social manipulation should receive analogous protection.

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

As stated above, there is a profound, yet easily implementable, step to address this manipulation. Government can extend the existing regulatory requirements to act in the best

interest of the data subject that apply to religious leaders, doctors, teachers, lawyers, government agencies, and others who collect and act on individuals' intimate data to also apply to data aggregators. Without any market pressures, data brokers who hold intimate knowledge of individuals need to be held to a fiduciary-like standard of care for how their data may be used, not least because inferences data traffickers make based on a mosaic of individual information can constitute intimate knowledge about who is vulnerable and when they are vulnerable.[45]

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

Barriers to entry exist in many digital markets due to network effects (the value of services rise with the number of users) and a range of other factors. The resulting power asymmetries should be treated more analogously to the regulation of natural monopolies offline.[46] Many jurisdictions, including the EU (via the Digital Services Act), have begun the process of legislative reform to re-establish the conditions for effective competition in these markets.

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

Governments can establish a governance structure along the lines of GAAP (Generally Accepted Accounting Principles) to regulate data traffickers and ad networks to ensure individualised data are not used to manipulate. Recently McGeveran (2019) called for a GAAP-like approach to data security, where all firms would be held to a standard similar to the use of GAAP standards in accounting. However, the same concept should also be applied to those who hold user data, regarding how they protect the data when profiting from it.[47]

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 require 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 capitalising on their vulnerabilities. A GAAP-like governance structure could be flexible enough to cope with market needs while remaining responsive and protecting individual rights and concerns.

Proposal 4e: Ensure that AI actors adopt and promote proposals 1-4, not only in the application of AI systems to personal data, also in but the collection and use of personal data in machine learning datasets which underpin the development of AI.

In the fast-growing and presently opaque development of AI systems, actors should reinforce data subjects' control of access to their O-Data and P-Data and the transparency of collections of such data, secure data collectives' control of their C-Data and tackle digital power asymmetries.

Where inferred data about people is used in a learning dataset for machine learning purposes, it is often to improve the outcomes for the data holder. The application of the principles above – especially principle 2c (on second-party P-Data) – will mean that the AI application should also

[45] 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.

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

[47] 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.

improve the outcomes for the data subjects and people like them. In applying the principle that second-party P-Data should be used always in the interests of the data subjects, AI developers will be encouraged to pursue ethical approaches to the use of AI. Further, the application of this principle will also have a positive impact on the integrity and methodology for compiling learning datasets. Not only will the question of bias need to be addressed in the selection of learning datasets, but also the best interests of the data subjects (including their human rights and the protection of data commons and the associated common-pool resources). For instance, a company seeking to build an AI program to protect it from customer fraud would have to consider whether the learning dataset is sufficiently diverse to ensure that the collection and use is in the interests of the data subjects, and/or that it is covered by specific public interest exceptions established by regulation. For example, perhaps information in a set limited to criminals only would not result in the data subjects agreeing that it is in their best interests.

This approach to AI is consistent with the principles for Artificial Intelligence and algorithmic ethics outlined recently by several prominent international bodies, such as the principles for responsible stewardship of trustworthy AI agreed by the G20 in 2019. The ethical governance for AI and its underlying Big Data has been discussed at national and dispersed international fora for several years, including efforts by the Organisation for Economic Co-operation and Development (OECD),[48] the Council of Europe,[49] the Innovation Ministers of the G7,[50] and the European Parliament.[51] In June 2019, the Group of 20 (G20) Trade Ministers and Digital Economy Ministers adopted a set of AI Principles[52] that draw from the OECD's principles and discussion of proposals from G20 engagement groups.[53] In November 2021, UNESCO gained the approval for its Recommendation on the Ethics of Artificial Intelligence from its 193 members[54] (UNESCO, 2021).

The principles underlying these initiatives point to a more human-focused and ethical approach for guiding AI. They include that AI actors must commit to respecting human rights, especially in regard to personal and collective dignity, autonomy, privacy, security, and inclusiveness. Furthermore, AI actors should implement safeguards and procedures that ensure the transparency and explainability of AI systems, as well as the security, safety and robustness of these systems throughout their lifecycles. Importantly, AI actors must be made accountable for the functioning of their AI systems.

---

48 https://www.oecd.org/going-digital/ai/principles/

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

50

51 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

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

53 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/

54 UNESCO has been called to support member states' implementation of this Recommendation and to develop an Ethical Impact Assessment and a Readiness Methodology.

Emerging regulation of individual-controlled digital identities

Proposals 1-4 build on a growing international consensus on the importance of individuals having and controlling their digital identities.

In April 2021, the Monetary Authority of Singapore (MAS) launched a report on the foundational digital infrastructure necessary for an inclusive digital economy and seamless cross-border transactions around the world. The first of four underpinning pillars was *Digital Identity* to ensure authentication and validation of an individual's identity, while protecting privacy and security of information.[55] Two months later the European Commission also proposed a framework for an EU-wide secure digital identity.[56]

In 2019, the Australian government passed legislation to implement "an economy-wide right for consumers to access and use data that businesses hold about them… and to authorise secure access to their data by accredited data recipients…. The consumer data right is a right for consumers to authorise data sharing and use. Consumers will determine which data is shared under the right, on what terms and with whom."[57]

The Australian regime is seen as having security and competition benefits. It has been implemented in financial services first, with the energy sector to be next. It is an opt-in regime whereby a consumer can choose to share her existing banking data (for example, her transaction history, interest rate and account balances) with a prospective bank or Consumer Data Right-accredited finance-related app or website.[58]

[55] See *Foundational Digital Infrastructures For Inclusive Digital Economies*, Monetary Authority of Singapore, April 2021 https://www.mas.gov.sg/-/media/MAS/Fintech/FDI/Foundational%20Digital%20Infrastructures%20for%20Inclusive%20Digital%20Economies.pdf

[56] See https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

[57] The Hon. Josh Frydenberg, MP, Treasurer, Second Reading speech on the Treasury Laws Amendment (Consumer Data Right) Bill 2019 to the House of Representatives, *Hansard* Wednesday 24 July 2019, p. 819

[58] See https://www.cdr.gov.au/

4. Implementation of the proposals

This chapter outlines in detail how the proposed policy framework could be put into practice through a set of implementation and audit models which draw on existing technical and business models used in the Internet's Domain Name System and in e-commerce. These principles are "doable". The technologies and business experience already exist to enable this scale of change. There are also proposals to mitigate asymmetries of information and market power.

Establishing a large-scale O-Data look-up system

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.

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 websites being presented. Consider that the loading of one page of an e-commerce website can result in more than 50 DNS requests – all of which resolve in a fraction 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. To support our policy proposal regarding O-Data, we envisage a data look-up and download system that would run on existing DNS infrastructure and processes.

The customer-facing service is run by many registrars, while the storage of the core DNS data and the managing of high-speed resolution of queries to that DNS data is handled by a smaller number of registries. The resolution process is very quick and highly scalable. The DNS also supports encryption of data queries. The *registrar function* could help attract consumers to join their service, help them have their record authenticated by trusted parties, and then negotiate terms for access on their behalf, while the *registry function* would focus on security and speed of data queries, including ensuring the attachment of specific transaction certificates or hashes to each request for O-Data. Just as in the DNS, there would be a search mechanism to find where one's record is and enable requests to access.

The registry function, including storing the records and maintaining the security of the data at rest, could also draw lessons from the current Payment Card Industry Data Security Standard model in North America. After several notorious data hacks of credit card data from retailers, the industry changed structure so that stores no longer maintain credit card information. Instead, once the customer supplies her credit card information, the seller passes it to another specialist provider who maintains all the information about the customer's credit card. The credit card processor is responsible for data transmission and security; it processes the payment and sends the confirmation back to the store. The security standards followed by credit card processors are detailed and now world-leading. A similar approach could be taken for the storage of O-Data.

While the 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[59] and DECODE.[60] A further range of technologies and processes – such as aspects of self-sovereign identity systems (see Annex 2) and Personal Information Management Systems (PIMS, see Annex 3) – are also relevant to the implementation of proposals 1a and 1b.

Regulatory amendment

Proposal 2c (using second-party P-Data exclusively in the interests of the data subjects) can be implemented through laws governing the integrity and confidentiality of second-party relationships, such as doctor-patient and lawyer-client, as well as the technologies mentioned above.

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 first three proposals above.

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.

[59] See https://www.specialprivacy.eu
[60] See https://decodeproject.eu
[61] For details on how this can be done, see Rannenberg et al. (2015).

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, in which transactions are associated with the citizenship of the individuals involved.

Control of personal digital data and diminishing the scope for manipulation

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.

A reallocation of control is fundamental to making the digital governance regime work in the interests of the digital consumers. First-party privy digital data has the same relevant characteristics as 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 right to control the data they generate. On this account, proposals 1-3 require that data subjects be given control over their first-party P-Data, that second-party P-Data be used in the interests of the data subjects, and that C-data be used in the interests of the members of the data commons. This means that the second parties should act as if the data subjects were in control of their personal data, provided they had the same information as the second parties. Proposal 3 also 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 – who collect, aggregate, and sell consumer data – are the engine of manipulation of online consumers yet have no interaction, contract or 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 of the actors. For example, Europe's General Data Protection Regulation (GDPR) 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

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

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," personal digital autonomy should be explicitly recognised as a legal right, as noted above.

Protecting such 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 digital 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 be held responsible for how their partners (ad networks and media) treat their customers and thereby make sure their customers' interests are being respected.[63]

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".

Handling the O-Data and first-party P-Data system: The technical digital architecture

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;

[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).

- authorisation for access according to negotiated terms;
- companies implementing their initial official data request;
- companies ensuring up-to-date upgrades to the data; and
- the auditing of companies to ensure the use of official data is consistent with the regime set out above.

Authentication

The first step is that a service provider (who could be a private 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 recognised bodies. This authentication would be in the form of a signed document 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 authorisation in a sub-jurisdiction, a governmental body (such as 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 certifications.

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 the transfer of data in a very short time, is similar in scope and capabilities to DNS registries.

If the proposed system is supported by governmental or other recognised trusted bodies for authentication, a distributed and fast-transacting database system will better service the technical and policy requirements than a relatively slow and expensive transaction on a blockchain system. Another reason for preferring a database system capable of authorised 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]

---

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

[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.

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.

Obligation

The further principle is **obligation**. Just as in offline 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 to be able legally to source it from the citizen-controlled records with the digital certificates, noted 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 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 will be necessary for the service provider to digitally watermark or fingerprint the record to say from where the record has come. This provision is additional to the layers of digital certification outlined above. The legal structure to support this obligation would also require entities which receive O-Data from another source not to use it and to report the source to authorities (similar to the regime concerning receiving stolen property).

Authorisation

The next stage is **authorisation** – who has the right to access these records and on what terms. This is the crux of re-empowering 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 (usually) 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 that 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 offline 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 specialisation in negotiating the best tailored terms with various types of data collectors. Some of these terms will be financial, many may not be.

While some individuals or agents may wish 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. For example, an individual could opt that O-Data always has to be validated but opt for pre-validation of P-Data bundles.

This new arena for collective bargaining could attract law firms, mutual funds or cooperatives, trade unions, consumer unions or for-profit companies. In practice, there could be a range of organisations seeking to be an individual'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 authorisation 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 individual could pre-enable a company to access the O-Data by giving instructions to the registrar type service provider – or permission could be given through an out of channel communication – the individual gets a prompt on her phone, like one does with credit cards, saying "this company is requesting this data about you, associated with your permissions, do you agree?" And then the person clicks on the phone app, or a text message or similar saying, "Yes, I agree." Then that transaction is complete, and it has been audited all the way through. Of course, it should also be encrypted all along the way.

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

The data service provider would also attach a tag/electronic certificate to at least part of the data being shared saying "this is O-Data" or "this is P-Data." Using similar technology to existing digital rights management, this tagging will enable receiving servers to determine if it is the sort of data their users can access, or to decide if this is data which should not be received. In this respect it would be similar to the classified document regimes used by governments which only allow delivery depending on the classification of the material.

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 databases;
- an auditable record of what official data can be accessed, how it may be used and by whom;
- a disincentive to sideways selling of 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 authorised use terms and certification, not in the personal information itself.

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

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 the individual specifically and find out who their nominated service provider is – 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 the collection of such data or to set conditions (including financial conditions) under which it is collected.

Updates

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 **update** 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).[67] 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 providers.

An **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 training to ensure they can analyse whether 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.

[67] 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.

The implementation of the users' right to directly manage and control their first-party P-Data will build on the system established above for O-Data. First-party P-Data (photos, geo-location data, biometric information, etc.) is placed online by the user in the context of a contractual or other legal relationship with a company (a cloud operator, telco, app provider, employer, etc.). This legal relationship will require the company also to hold the individual's O-Data as part of their account management processes. The individual or her collective bargaining agent will negotiate financial and use terms for first-party P -Data as part of the right for accessing the authoritative 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 laws requiring that P-Data be held and used in the interests of the data subject.

Drawing on emerging models to benefit consumers and business

Considering the steps laid out above, it is important to recognise that existing and in-development technology could be leveraged for practical implementation.[68]

On O-Data, a single, verified source of data would result in a significant reduction of duplication – both for consumers and for businesses. The second-order effect of this is that the consumer burden of continuous update across an ever-increasing number of providers is reduced, retention of out-of-date data is reduced, and resultant errors or disclosures are also reduced.

The implementation of the above recommendations could also draw on the lessons of Personal Information Management Systems (PIMS), and the related Personal Data Stores (PDS), which have been implemented on a modest scale to improve the portability and interoperability of systems using personal data.

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.

A Personal Data Store lets a user store all their own personal data, whether on a device they directly control, or on 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. One project developing such tools is Solid, which was co-founded by the inventor of the Web, Tim Berners-Lee.[69]

In some implementations, such as Databox,[70] 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.

[68] Professor Ian Martin, Scarlett McClure and Maria Farrell contributed significantly to this section.
[69] https://solid.mit.edu/
[70] https://databox.com/

Some potential benefits of PIMS and PDS include:

- Enabling 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 erase data.
- Acting as identity providers, enabling an individual to log in to many different websites while protecting their privacy.
- Acting as a secure backup of users' personal data.
- Facilitating micropayments for services that require it, in addition or as an alternative to providing access to personal data for advertising and other purposes.

The Finnish government has supported the development of a MyData framework implementing a personal information management system. The framework principles are shown in the following table (Poikola, Kuikkaniemi & Honko, undated).

1. Human-centred 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, standardised 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 for society.
3. Open business environment: Shared MyData infrastructure enables decentralised 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.

There are now national MyData hubs in 40 countries, with nearly 100 organisational members.[71]

A potentially highly valuable deployment for businesses as well as consumers could be one in which a service provider may temporarily access data, perhaps in a cache or similar, but is never entitled to duplicate or store the O-Data data owned by the subject. A read-only solution such as this would almost eliminate instances of aggregate data breaches – a leading cause of identity theft and digital consumer exploitation. There must be consideration for latency and a common definition of terms in such a solution.

Existing SSO technologies achieve the PIMS function to an extent, however, they tend rely on centralised storage and ownership of data by third parties who may themselves be breached, and most often some O-Data is still recorded by the service utilising the SSO. A solution whereby each individual has a PDS and access to the data is administered through a decentralised transaction system, would provide a transparent record of access while affording the subject the ability to govern access using smart contracts. This could be extended to govern P-Data also but would require an extreme level of availability and transfer speed to apply to services like image or video sharing platforms.

[71] https://mydata.org/hubs/

Imagine a scenario in which users are able to define a legal contract with any party wishing to access their data without the need for lawyers or time-consuming intermediation.

- A consumer may define that they wish to remain anonymous for particular interactions.
- A consumer may define those certain elements of their data that are accessible to a particular service provider but stipulate precisely which fields and any rules regarding retention and expiry.
- A consumer may determine which elements of their data are available on demand for a virtual “data commons”.
- A consumer may define what, if any, payment must be made to them for access to their data under certain terms.

Such a system would be a significant move in the direction of the free data market defined in the report, while affording users improved privacy and security. By governing such a system through smart contracts – combined with a carefully designed User Interface (UI) in order to make data governance accessible to everyday users – the need for complex and highly resourced governing bodies is reduced. Automated compliance auditing may be developed.

In combination with maturing data-fingerprinting and encrypted processing technologies, these systems could be further secured through unique encryption for each transaction.

A potential business eco-system to support the O-Data and first party P-Data system

This paper foresees a business ecosystem to implement these proposals which would likely have a market structure similar to the mature Domain Name System (DNS) or the credit card processing industry. The consumer is likely to engage a consumer-facing services enterprise that manages the details of consumer preferences and negotiates terms on behalf of consumers. The consumer-facing enterprise would pass the registration of the consumers details to a specialist, secure data holder and processor, which would manage the requests for the consumer’s data from the myriad of entities with whom the consumer interacts according to the terms set by the consumer.

In the DNS, these functions are undertaken in most markets by separately accredited registrars and registries.[72]

A domain name registrar is the customer-focusing service that enables the consumer to reserve domain names as well as the assignment of IP addresses for those domain names. Many registrars also offer other services such as website development, hosting and email. For country codes, registrars operate under accreditation by the county code operator for the provision of the two-letter country code domains (e.g. .uk, .de, .au) and from the multistakeholder Internet Corporation for Assigned Names and Numbers (ICANN) for generic top-level domains (e.g. .com, .net, .org).

The registrar pays fees to the registry operator for each web address registered through their service.

The role of the registry operator is to keep the authoritative database of all domain names registered in each top-level domain (TLD) and generate the “zone file”, which contains all of the delegations for that top-level domain, as well as the list of root servers, allowing computers to route Internet traffic anywhere in the world.

[72] In some country codes, such as Brazil (.br), the two functions are done by the same entity.

We can envisage a similar structure for personal data management with registrar-type bodies recruiting consumers and producing various degrees of specialisation and services in negotiating terms for the use of that data. The details of the consumers' O-Data and related terms for access, including first person P-Data, and access rules would be passed to the secure data-holding registry for hosting and for managing the authorisation process when a data requester wants the consumer's personal data.

The registrar would be responsible for ensuring that the consumer's data is up to date, and the registry would ensure that requesting entities have access to up-to-date upgrades to the data.

Considering the huge scale of covering all consumers, and drawing from the experience of the DNS, we expect that the operational cost of the registry function would be a dollar or less per year. There would be significant capital costs in establishing a registry, but existing large-scale data processors would be in a strong position to establish a sister registry business. The cost of the registrar function would vary according to scale achieved by each registrar and the resources they dedicate to negotiating terms for consumers. We would expect both registrar and registry businesses to be competitive organisations. Overall, it is feasible that the annual cost to the consumer for these services could be similar to that of a take-away coffee.

Means to enable collective representation[73]

These proposals foresee expert entities representing the interests of users in proposing and negotiating options of data sharing and benefit sharing in return for access to users O- and first party P-Data. This is important if the handling of billions of people's personal data is to shift from digital husbandry to a more properly operating market in which the users are participants. Presently, those with skills in how data aggregation, analytics and online advertising processes work overwhelmingly serve the data aggregators and the influencers. It is not feasible that each user should ascertain this knowledge – hence the benefit of collective representatives who can bring similar skills to the interests of users. George Akerlof (1970) famously pointed out how information asymmetries undermine markets. And skilled people are essential to bringing information to both sides of a properly operating digital market. In this way, we envisage that some lessons of how collective representation of workers changed the labour markets in the nineteenth and twentieth centuries will be instructive in the personal data market of the twenty-first century.

So what is the potential for existing entities such as trade unions, lawyers, registrars, cooperatives or other groups to develop into this space? Will we need digital-data versions or manifestations of fundamental international standards on freedom of association and collective bargaining? Are there things that can be replicated or applied from that experience, and even from that jurisprudence?

Freedom of Association (Convention 87) and the Right to Organise and Collective Bargaining (Convention 98) are "core" Conventions of the ILO. They are widely ratified but also widely violated by States directly and by States failing to ensure they are respected. Workers and employers are allowed under these Conventions to create and join associations. They have accrued a large amount of jurisprudence under the ILO's supervisory mechanisms, notably the Committee on Freedom of Association and the Committee of Experts on the Application of

[73] This section was significantly contributed to by Tim Noonan.

Conventions and Recommendations, which provide the basis for decisions by the ILO Conference and the ILO Governing Body.[74]

These Conventions apply in employment situations, where a relationship between a worker and an employer exists. As mentioned above, they are under threat in the “gig economy” or “platform businesses” due to employers denying that an employment relationship exists (governments and courts are beginning to overturn this). One issue here is that “gig” workers may work for more than one employer. This is analogous to some types of freelance worker, where in fact (journalists, musicians, actors etc.) often have relatively high rates of unionisation and negotiate collectively for industry standards including pay rates. However, in some countries, competition law is used to stop freelance workers bargaining collectively because it is deemed as cartel behaviour.

Trade unions generally admit members from particular occupations, sectors, and in some cases those who work for particular employers. There are also general unions which have broader eligibility criteria.

In the labour market, freedom of association is based on the contractual relationship between the worker and the employer. Freedom of association for digital users would take another form – perhaps becoming a user of a digital provider could constitute the threshold for becoming a member of a user association. The ILO Conventions provide wide discretion for how unions and employer associations constitute their rules and procedures and protect this from State interference. Unions operate on the basis of fees paid by their members in order to ensure independence from employers and governments.

Presumably, digital users’ associations would themselves predominantly operate on a digital basis. They could be organised according to provider (“Google Users’ Association”) but ideally would be organised and bargain with associations of digital providers. In the employment context, there are often sectoral or industry agreements negotiated, with additional “top-ups” negotiated for particular enterprises in addition to the industry agreement.

The legislative framework around workers’ freedom of association and collective bargaining is extremely important. Analogous frameworks would need to be created for digital user associations (trade unions could provide advice on key aspects of that), potentially with different provisions concerning C-, O- and P-Data.

Managing the data commons

A personal data commons refers to personal data that is associated with 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.

[74] See https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C087
https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312243

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 (Sanfilippo, et al., 2018). Data commons allow people to use their rights of association 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 for the public good" described above, different types of data commons will include:

- Data commons established by, for example, 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 (Noble, 2018; Criado Perez, 2019). 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.

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,[77] 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.[78]

[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] https://www.ft.com/content/e5c5a996-8d54-4d5c-a5df-a036b5579148

[78] 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 women's (walking). See

- 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.[79]

Principles for managing the data commons

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 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.

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:

1. Each data commons should be defined by a clearly articulated purpose, supported by a shared identity of the data commons users.
2. The contributions to and benefits from the data commons must be equitably distributed among the users.
3. The decisions concerning the management of the data commons should be fair and inclusive in the eyes of the users.
4. User behaviour should be monitored.
5. Helpful and unhelpful behaviours should be met by graduated rewards and graduated punishments, respectively.
6. Fair and fast conflict resolution mechanisms should be available to the users.
7. The decision-making authority of the users must be respected by third parties.
8. Where there are synergies to be exploited across different data commons, collaborative relations among different data commons should be promoted through polycentric governance.

Criado Perez, 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.

[79] 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.

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.

A first policy move

In December 2021, the European Council and the European Parliament reached a provisional agreement on a new Data Governance Act (DGA) to build a trustworthy environment to promote the sharing of data to facilitate its use for research and the creation of innovative new services and products.

There are four pillars to the DGA:

- a mechanism for re-using certain categories of protected public-sector data which is conditional on the respect of the rights of others (notably on grounds of protection of personal data, but also protection of intellectual property rights and commercial confidentiality);
- establishing a framework for new data intermediaries to increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data;
- encouraging data voluntarily made available by individuals or companies for the common good (data altruism), establishing the possibility for organisations engaging in data altruism to register as a "Data Altruism Organisation recognised in the EU" in order to increase trust in their operations; and
- fostering coordination and interoperability through the European Data Innovation Board.[80]

To build confidence in data sharing between organisations and individuals, access to data they agree to share is to be facilitated by third-party data-sharing service providers. This role is similar to the "data trusts" concept discussed in the UK and other Common Law jurisdictions.

These data intermediaries will be required to maintain neutrality and comply with strict requirements, including not being permitted to use the data for their own interest. A certification or labelling framework is proposed along with a notification obligation with subsequent

[80] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) COM/2020/767 final. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

monitoring of compliance with the requirements by designated competent authorities within member states. These proposals are not applicable to closed-group data-sharing initiatives.

These data intermediaries will be required "to remain neutral as regards the data exchanged. They cannot use such data for other purposes. In the case of providers of data sharing services offering services for natural persons, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met. The approach is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services."[81]

This draft act does seek in general to meet many of the objectives we outline above with respect to data commons. There remain some uncertainties about the draft act in its definitions and implementation and application to non-European entities.[82] For instance, the European Consumer Organisation has stated, "We are concerned about how a weak definition of altruism in this agreement could allow companies to over-use vague, altruistic grounds to push consumers to share their data."[83]

But overall, it would appear to be a promising first step. It will be interesting to see how other jurisdictions respond.

Building on existing security standards

Securing how the three types of user data are 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 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 centres storing user data will need to be SOC-2[84] and GDPR compliant. This requires data centres 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)[85] 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 behavioural data. These examples provide a clear connection to user data as defined by O-, C-,

---

81 *Ibid.*

82 For more details see as examples: https://www.pinsentmasons.com/out-law/analysis/the-eus-data-governance-act-just-part-data-sharing-puzzle ;

83 Quoted in https://www.euractiv.com/section/digital/news/data-governance-new-eu-law-for-data-sharing-adopted/

84 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

85 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

and P-Data. In addition to the guidance on PII, when storing user data that contains medical information, the GDPR and HIPAA[86] 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 takeaway 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 do they want the responsibility of meeting PCI compliance. As a result, specialist companies have developed and maintained data centres that meet PCI compliance and specialise in these transactions. These companies provide a passthrough for the commercial entities to process the credit card transaction on their 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 specialised in meeting the standards described above for storage and processing of user data.

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

5. Implications of implementing the proposals

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

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.[87]

A recent study of 1 million websites 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 information such as usernames, addresses, emails, and spending details. The latter allow data aggregators to then de-anonymise much of the data they collect (Englehardt & Narayanan, 2016; Libert, 2015).

[87] 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/ .)

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.[88] 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 organisation 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 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 digitisation 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, & Nissenbaum, 2019). Offline, we regulate manipulation similarly 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 allow 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.

[88] 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).

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 & 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 & Goldstein, 2003; Sunstein, 2017; Thaler & 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.[89] 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.

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.

[89] Facebook recently offered advertisers the ability to target teens when they are "psychologically vulnerable".

Digital trade[90]

Data governance and the governance of cross-border data flows are different but intersecting areas of policy. International trade is not the main concern of this proposal, which initially focuses on the treatment of data at the national or regional level. However, data flows between countries have reached a voluminous scale and continue to increase. They can therefore not be ignored in this discussion. Cross-border data flows underpin and make possible trade in digital form. This “digitalisation” is estimated to account for 50 percent of traded services and around 15 percent of traded goods. However, data flows on their own are not statistically recorded in an accurate manner, if at all, and thus we do not have an accurate grasp on either their current magnitude or their potential magnitude.

Data flows and data in general have become vital to international trade. Data flows, especially those that enable trade in digitised goods and services, have had a strong impact on both trade and economic growth. A now somewhat-dated report by the McKinsey Research Institute estimated that cross-border data flows raised the level of world GDP by 10 percent over the decade 2005-2015, as much as the contribution of trade in goods and services (Manyika, Lund, Bughin, Woetzel, Stamenov & Dhingra, 2016). The ability to move data globally is contributing to the development of new business models, spurring research and development and facilitating international collaboration in many areas, including a collective response to the Covid health crisis.

Firms depend upon their ability to transfer data, and many can only maximise the value of their operations when data can flow freely across borders. Impeding data flows through restrictive policies has a particularly detrimental impact on small and medium-sized firms that do not have branches or subsidiaries abroad and are thus cut off from trading in those countries with burdensome restrictions where they may have or wish to develop customers. Thus, data governance regimes can effectively turn into “data protectionism”, depending upon how they are designed and implemented.

The trade rules that have been included in Preferential Trade Agreements (PTAs) or in recent standalone digital agreements have an impact on data flows, to the extent that they discipline some of the barriers that are being put in place to impede them, including, in particular, data localisation requirements and restrictions on data flows. Data localisation rules require companies to store a copy of the data they collect and use locally, and to process data locally. Government consent is often required for data transfers, which takes the form of restricting cross-border data flows.

Cross-border data flows will thus be influenced by the type of legislation that is adopted at the national level to protect the personal data of citizens or ensure national security and other interests determined to be vital to the state. There is thus a strong interconnection between cross-border data flows, trade rules on digital trade issues and national data governance regimes.

As the table below shows, the current divergent approaches to the treatment of data, from the greater to lesser stringent protection regimes for personal data, to the varying definitions of what

[90] This section was significantly contributed to by Sherry Stephenson.

constitutes national security and “important” data, have meant that the international economy is being fragmented into data governance silos that effectively “balkanise” the use and location of data. Many studies have shown that excessive restrictions on cross-border data flows will impact on the ability of international trade to contribute to potential economic growth and greater efficiency in the world economy. Restricting data flows “per se” through a recourse to data localisation requirements has also been shown to reduce innovation and scientific collaboration, among others.

Provisions in recent trade agreements addressing privacy for personal data and consumer protection

Provision:	CPTPP March 2018	US-Japan DTA October 2019	USMCA December 2019	DEPA June 2020	AU/Sing Digital Economy Agreement December 2020	EU-UK TCA December 2020
Does the agreement mention trust?	No	No	No	Yes	Yes	Yes
Enforce domestic laws regarding privacy	Yes	Yes	Yes	Yes	Yes	Yes
Enforce domestic laws regarding consumer protection	Yes	Yes	Yes	Yes	Yes	Yes
Enforce domestic laws regarding spam	Yes	Yes	Yes	Yes	Yes	Yes
Cooperation on cybersecurity	Yes	Yes	Yes	Yes	Yes	Yes
Regulations banning divulgence of encryption	No	Yes	No	Yes	Yes	No

Table by Andrew Kraskewicz with S. Aaronson, Source: From Trade to Trust: A Different Approach to the Free Flow of Data across Borders, CIGI, August 2021

However, to date trade negotiators have refrained from interfering in national sovereign decisions on cross-border flows of personal data, and trade agreements simply mandate that governments put in place a system of consumer protection and that they enforce their own privacy laws. Only the more recent digital agreements encourage discussions of how to achieve “interoperability” of these privacy laws that govern the use and cross-border flow of personal data. A chart with comparative provisions in recent trade agreements addressing privacy for personal data and consumer protection is set out above. While these trade agreements only mandate the enforcement of domestic laws on privacy of personal data, consumer protection

and spam, several include regulations banning the divulgence of encryption and mandating cooperation on cybersecurity. Discussions on achieving interoperability of data governance regimes are, however, not mandated.

The main concerns for trade policy officials and analysts with respect to digital trade are twofold. The first is to ensure that the WTO agreement is "modernised" and made fit to purpose to serve the needs of the digital world through an updated set of trade rules. Making expeditious progress in the current plurilateral negotiations on E-commerce under the Joint Statement Initiative being carryied out at the WTO is very important in this regard. The participating 86 WTO members in the negotiations would encompass the largest number of countries signing onto a trade agreement covering the digital economy and would be an important step towards reducing the risk of such balkanization. There are many issues for which binding disciplines are being sought, including the guarantee of cross-border data flows, the recognition of digital or e-signatures, authentication, prevention of spam (unsolicited personal communications), the validity of electronic contracts, online consumer protection and the prohibition of data localisation requirements, among others. Binding rules aim to limit restrictions or discrimination to occasions and objectives that are legitimate and genuine, in order to make digital trade and data flows more stable and predictable.

The second concern of international trade officials and analysts is to ensure that national regimes for protection of personal data are not overly restrictive in fulfilling what are legitimate objectives for the protection of citizen privacy, as well as national security, and that these data governance regimes can be made interoperable. A guide for thinking about the former element is the WTO Sanitary and Phytosanitary Agreement that provides a useful article on the need to avoid measures that are "not more trade-restrictive than required to achieve their appropriate level of ……protection" (Article 5.6). as Also relevant is an article on the requirement to "….take into account the objective of minimizing negative trade effects (…when determining the appropriate level of sanitary or phytosanitary protection)" (Article 5.4). The Agreement on the Application of *Sanitary and Phytosanitary Measures* (SPS Agreement) allows countries to set their own standards. But these should only be applied "…. to the extent necessary to protect human, animal or plant life or health. And they should not arbitrarily or unjustifiably discriminate between countries where identical or similar conditions prevail……". One could substitute "personal data" in this case for human life or health.[91]

There have been continued concerns following the EU's most recent regulatory initiatives – the Digital Markets Act (DMA), the Digital Services Act (DSA) and the Artificial Intelligence Act – that the further detailed cementing of privacy rights by one major international player will impede international trade agreements (for instance, Kyvik Nordås, Lodefalk & Wernberg, 2021). One of the benefits of the proposals in this report is that consumers gain real control over whether and what data about them companies and other entities can collect – and for what purpose. Individuals gain control of making decisions about how much privacy they want and in return for what benefits. Such a market-based system – where the individual is a properly empowered and represented market participant – should be consistent with the thrust of international trade agreements. This does not vitiate the need for regulatory support for privacy nor for the establishment of the system we outline. But as digital markets change, consumers, as full market participants can amend their terms – taking the pressure off legislators in some regions, who feel the need to play the sort of regulatory catch-up that would undermine trade agreements.

[91] https://www.wto.org/english/res_e/booksp_e/agrmntseries4_sps_e.pdf

The need to make the different data governance regimes interoperable is of vital importance as well in the world economy. This is a challenging task, as it must somehow find a way to breach different conceptual treatments of personal data as well as the practical application of conditions. The two main regional groupings that have developed schemes for data protection, namely the EU through its General Data Protection Regulation (GDPR) and APEC, through its Cross-Border Privacy Rules (CBPR), operate on the basis of "adequacy" rulings for the former and "accountability" assessments for the latter, which are quite different approaches. The proposal in this study for adoption of a human-centred approach to the treatment of personal data would build upon and extend the EU's GDPR. The two schemes can conceivably be made compatible, but it will require behavioural changes on the part of firms and most likely the negotiation of contractual clauses that could be adopted and recognised by both groupings. It would also be imperative to open up the GDPR and the CBPR schemes to outside countries in order to foster a broader basis of adherence to an agreed interoperable system that would permit the compliant flows of personal data.

It may be questioned, however, whether trade agreements are the best place to discuss/ negotiate digital issues, including interoperability mechanisms for data privacy regimes, cyber security concerns and the social impacts of new digital technologies on disinformation and consumer behaviour. Trade negotiators aim to finalise binding rules. Many of these delicate and complex digital issues require a lengthy process of discussion and cooperation among national regulators before understandings can be reached. New issues may require a trial-and-error approach before settling upon the best common way forward. This argues against consolidating rules in treaty form until they are fully sorted. The recent standalone digital agreements (the Digital Economy Partnership Agreement of June 2020 and the Australia-Singapore Digital Economy Agreement of December 2020) may provide better models for addressing many digital issues in a modular way so that regulators can carry forward the discussions in an exploratory manner before attempting to reach binding disciplines. Consolidating the consideration of digital issues into one agreement, including rules on digital trade, may be the new (and preferable) path forward.

Addressing these challenges in the international trade arena and elsewhere will be of immense importance in the near future, to ensure that the trading system is responsive to data-driven developments in the 21st century economy, to curb and redress the proliferation of restrictive measures around data and other digital issues, and to prevent the deepening of data silos and the balkanization of data governance regimes in the world economy.

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 summarised, 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 channelling 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.

Privacy

In their most recent *Freedom on the Net* report, Freedom House calls for, *inter alia*:

"**Enact robust data privacy legislation.** Governments should enact updated legal frameworks that comprehensively safeguard user information. Individuals should have control over their information, including the right to access it, delete it, and easily transfer it to the providers of their choosing. Companies should be required to limit the collection of consumer data and disclose in plain language how they use it, as well as details on third parties that may access the data and how they are allowed to use it. Companies should be required to notify customers in a timely fashion if their information is compromised. Updated data privacy legislation should also provide a mechanism for independent verification of major foreign and domestic companies’ data-collection practices to ensure compliance with local laws on privacy, non-discrimination, and consumer protection. In the United States, lawmakers should pass a federal electronic privacy law that provides robust data protections, including for biometric data, and harmonises rules among the 50 states. The Federal Trade Commission (FTC) and other relevant agencies should be empowered to pursue privacy enforcement using existing authorities."[92]

The proposals in this report seek similar outcomes with the very significant benefit that once the market empowerment of the consumer is enacted, there is much less need for ongoing legislative amendment. Rather, consumers will be able to set the protections suggested above via their direct or representative's negotiations of terms of access.

The significant contribution to individuals’ privacy envisaged in these proposals is giving individuals real control over whether and what data about them companies and other entities can collect – and for what purpose. Individuals get control of making decisions about how much privacy they want and in return for what benefits. Rather than relying on overarching, prescriptive legislative tests, our proposals prefer a market-based system – but where the individual is a properly empowered and represented market participant. Further, as full market

[92] https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech/policy-recommendations

participants, consumers can amend their terms as the market changes – taking the pressure off legislators to play catch-up through regulatory “Whack-A-Mole”.

This market process will also incentivise companies to provide innovative services while also offering the individuals clearly defined and mutually agreed benefits. Unsolicited data collection on individuals would no longer be incentivised.

The proposals here require the creation of a secure, authoritative record of individuals’ data. But this is amounts to much less than the present circumstances in which every company, government agency or charity can establish its own avatar of an individual without that person knowing or ensuring that the information is accurate. Requiring that this consumer-controlled authoritative record be used by companies and others significantly reduces the incentive for the continued creation of such avatars.

Competition

The implementation of the above proposals would add an important market incentive for new players to enter the digital markets. Because they can offer shared benefits with their customers, new companies should be able to swiftly access significant, authenticated O- and P-Data on their customers. This, to a significant extent, will undermine the moats that existing data aggregators have built around their companies through unsolicited data collection.

For consumers, maintaining one authoritative record of O-Data will promote more convenient switching between products and providers.

For businesses, it will reduce the costs of maintaining accurate data on consumers. Further, products and services should speak for themselves to the consumers, rather than relying on hidden manipulation of consumer behaviour. Consumer data success will depend more on meeting the needs of consumers, negotiated by their representatives, rather than surreptitiously accumulating vast amounts of data about the consumer.

Innovation

As stated above, the incentive for companies to share benefits with consumers in return for negotiating access to more of their O- and P-Data should be a significant driver of product and service innovation as well as fuelling competition.

While the above proposals will certainly put a brake on unsolicited surveillance capitalism, they will also create opportunities for companies to offer services as citizen-facing registrars and representatives and also secure infrastructure providers to hold O-Data and resolve requests for access to it.

Europe has 32 country code operators within a single market. These operators alone could constitute an experienced platform of enterprises used to serving customers and resolving high-speed DNS queries. Europe also has experienced traditional and fintech data processors that could bring expertise to the new opportunities in holding securely personal data.

Impact on hate speech and misinformation

Countering hate speech online is often described as major policy challenge, because of the need to balance protecting individuals and groups from opprobrium without eroding freedom of speech. But this challenge is one which policy makers in nearly every country have addressed in the offline world over the last centuries – with differing outcomes in different jurisdictions.

The real challenge in the online world is the massive use of anonymisation to protect the identity of authors and commentators. Such anonymisation has its benefits for people seeking to pursue human rights under repressive regimes, but in open societies its significant beneficiaries are extremists, trolls and criminals.

Again, anonymisation is not new, and jurisdictions have well-established solutions for balancing the rights of the author and the slandered person in the offline world. Interestingly, governments are starting to apply these rules to the online environment. The United Kingdom imposes criminal penalties on hate speech, both online and offline through The Crime and Disorder Act, Public Order Act, Malicious Communications Act 1998 and Communications Act 2003 (see O'Regan & Theil, 2020). The German government has introduced the German Network Enforcement Law to ensure swift processing of complaints by platform companies. The Australian government will introduce new court powers to force global social media companies to unmask anonymous online trolls and enable individuals to file defamation suits in court. Again, a government is relying on established offline norms for balancing free speech and defamation. But in a move to counter blanket anonymisation, the Australian government will ensure social media companies are considered publishers and can be held liable for defamatory comments posted on their platforms. They can avoid this liability if they provide information that ensures a victim can identify and commence defamation proceedings against the troll. In other words, the rules that exist in the real world should exist online too.

Australian Prime Minister Scott Morrison recently said “Social media can too often be a coward’s palace, where the anonymous can bully, harass and ruin lives without consequence. We would not accept these faceless attacks in a school, at home, in the office, or on the street. And we must not stand for it online, on our devices and in our homes. We cannot allow social media platforms to provide a shield for anonymous trolls to destroy reputations and lives. We cannot allow social media platforms to take no responsibility for the content on their platforms. They cannot enable it, disseminate it, and wash their hands of it. This has to stop.” (Morrison, 2021)

The Australian government has secured support for global action to be discussed at the G20 in Indonesia in 2022.

Similarly, both sides of the political aisle in the US Congress are actively discussing the reversal of Section 230 of the 1996 Telecommunications Act, which provides online platforms and ISPs with immunity for liability from most content posted or transmitted by their users. While agreement is not yet apparent, the desire to remove blanket immunity is.

In the midst of these present moves to bring offline norms into the online environment, the proposals in this paper provide a user-empowered mechanism to allow for the identification of individuals who have a personal data link with enterprises. Companies will have an authenticated point of contact with customers.

Anonymisation

The question of being an anonymous actor on the Internet is a conundrum. There are civil society activists, political actors, trade union officials, journalists and health advocates in many jurisdictions for whom being able to browse and communicate anonymously is essential. On the other hand, such anonymisation disproportionately enables the malicious action of trolls, terrorists and criminals. In between, there are consumers in open societies who would prefer to not be identified in some online activities or communications.

Nothing in these proposals requires that consumers have to adopt real name and personal identifier handles for creating user-facing identities in online platforms or creating email addresses. These proposals apply only where the enterprise or public bodies seek the consumer’s O-Data or first party P-Data. It is foreseeable that some personal identity registrars and registries (as outlined in the model above) could choose to keep their consumers’ data in the citizens’ jurisdiction (a form of data sovereignty, even if not required by the local government). The analogy from the DNS is country code Top Level Domains (ccTLDs), which only register names for residents of the related country. In this case, consumers should have access to personal data service providers who offer services across borders – similar to the role played by generic Top-Level Domains for the DNS.

Recent amendments to the European Union’s Digital Services Act provide for the right to use and pay for digital services anonymously. This appears to be an outlier in national legislative frameworks, which require many companies to know their customers to help respond to threats from trolls, terrorists and criminals. It should be noted that responding to these threats is an agenda item for the G20 heads of government. At their 2019 meeting, the heads of government pledged: “Recognizing the responsibility of digital service providers, we will work in 2022 towards enhancing confidence in the digital environment by improving internet safety and

countering online abuse, hate speech, online violence and terrorism while protecting human rights and fundamental freedoms."[93]

Impact on human rights

The proposals above contribute in several ways to further the human rights of users.

Giving individuals control over who can access authoritative data about themselves and for what purposes (O-Data and First Person P-Data) allows them to exercise their rights and ensure that data aggregators and influencers are not seeking to undermine these rights, especially without the express understanding of the user. The creation of a regime which counters the unrestricted creation of avatars of individuals without their knowledge also limits the unknown profiling of people for political or criminal manipulation.

These proposals also reinforce the importance of several human rights, especially the Right to Free Association.

In considering the impact on human rights, we have focused on those outlined by the 1948 Universal Declaration of Human Rights. These could be expanded to include rights outlined in the nine core UN human rights treaties.[94] But even these expanded treaties are controversial in some quarters and can be seen as deriving from the basic 30 principles outlined in the Universal Declaration.

Of the 30 articles affirming an individual's rights, we consider that the proposals above positively reinforce the following principles:

12. Right to privacy

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

18. Freedom of thought and religion

Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

---

[93] *G20 Rome Leaders' Declaration* see https://www.consilium.europa.eu/media/52732/final-final-g20-rome-declaration.pdf

[94] See https://www.ohchr.org/en/professionalinterest/pages/coreinstruments.aspx

- the International Covenant on Civil and Political Rights (ICCPR)
- the International Covenant on Economic, Social and Cultural Rights (ICESCR)
- the International Convention on the Elimination of All Forms of Racial Discrimination (CERD)
- the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)
- the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT)
- International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW)
- the Convention on the Rights of the Child (CRC)
- the Convention on the Rights of Persons with Disabilities (CRPD)

19. Freedom of opinion and expression

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

20. Right to assemble

Everyone has the right to freedom of peaceful assembly and association. No one may be compelled to belong to an association.

21. Right to democracy

Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. Everyone has the right of equal access to public service in his country.

The rights above would be important contributions to the proposed interpretation of the "interests of the data subject" in proposal 2 c (dealing with second party P-Data).

Cybersecurity

One of the biggest vulnerabilities of online interactions is the false personification of individuals (real or imagined) in order to manipulate actions by other individuals or enterprises.

The proposals above establish, at least for businesses, a single point of confirmation for authenticated O-Data about an individual – controlled by the individual but authenticated by trusted third parties. This diminishes the risk of an individual lying about their O-Data.

Another benefit of attaching digital signatures/hashes to the transaction-related holdings of an individual's O-Data by an enterprise is that stealing a company's database of customer records would be far less valuable to criminals than it is today. Unlike now, such records would not be fungible – but specific only to that company and the transaction. The value of the database to other criminals for other uses, such as phishing, would be considerably diminished.

Aspects that would need to be managed include:

- Ensuring and auditing that the trusted third parties really do have a secure and trustworthy process for authenticating individuals' data.
- Recognising that holding a lot of personal data in one spot makes it a target for both criminal and potentially sophisticated national state actors. Hence the need to adopt the sort of specialised, high security management techniques that are now deployed by such actors as credit card processors. Sophisticated nation states have been accused of large-scale data breaches – but attacks on such sources as the US Office of Management and Budget indicate that state actors prioritise targets with a high level of contextual data about individuals. Data such as O-Data sets are already held by big customer-facing companies and platform companies. The proposals above for transaction-specific digital signatures would make these holdings more secure. But big holdings of C-Data could be attractive targets for state actors, e.g., large datasets on health data. Consequently, we would recommend that C-Data be held on similarly secure infrastructure as the O-Data providers.

How would the new model work

- Give Citizens control over who has access to the personally identifiable data they create
- Citizens set the terms under which their information can be used (citizens need to ensure that their data is accurate and verified by trusted third parties)
- Entities which want to use someone's personal data must access it only from a consumer-controlled data repository under agreed upon terms
  - Citizens can enable their interests to be represented by expert representatives
  - The data accessed has transaction specific digital signature confirming has been sourced correctly
- Entities which infer information from data which the citizen does not create will have to abide by the duty-of-care rule that commonly applies in the offline world - the data can only be used in the "best interests" of the data subject
- Governments will create the legal structures to support the establishment of data commons, where citizen communities with common interests who can pool personal data

6. Concluding remarks

The policy proposals above are to be understood as primary guidelines for giving digital consumers control, individually and collectively, over their personal data.

On their own, these proposals 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 those that promote the widespread acquisition of digital skills, bridge 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.

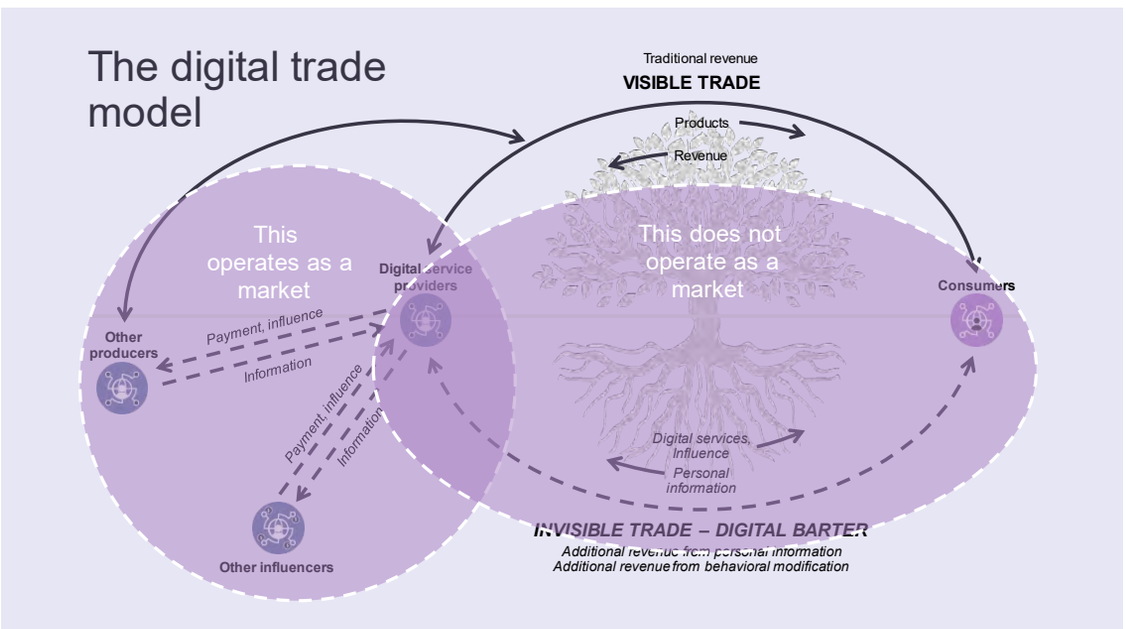
Fourth, the use of O-Data and associated use of P- and C-Data would significantly reduce a wide variety of cybersecurity and fraud threats.

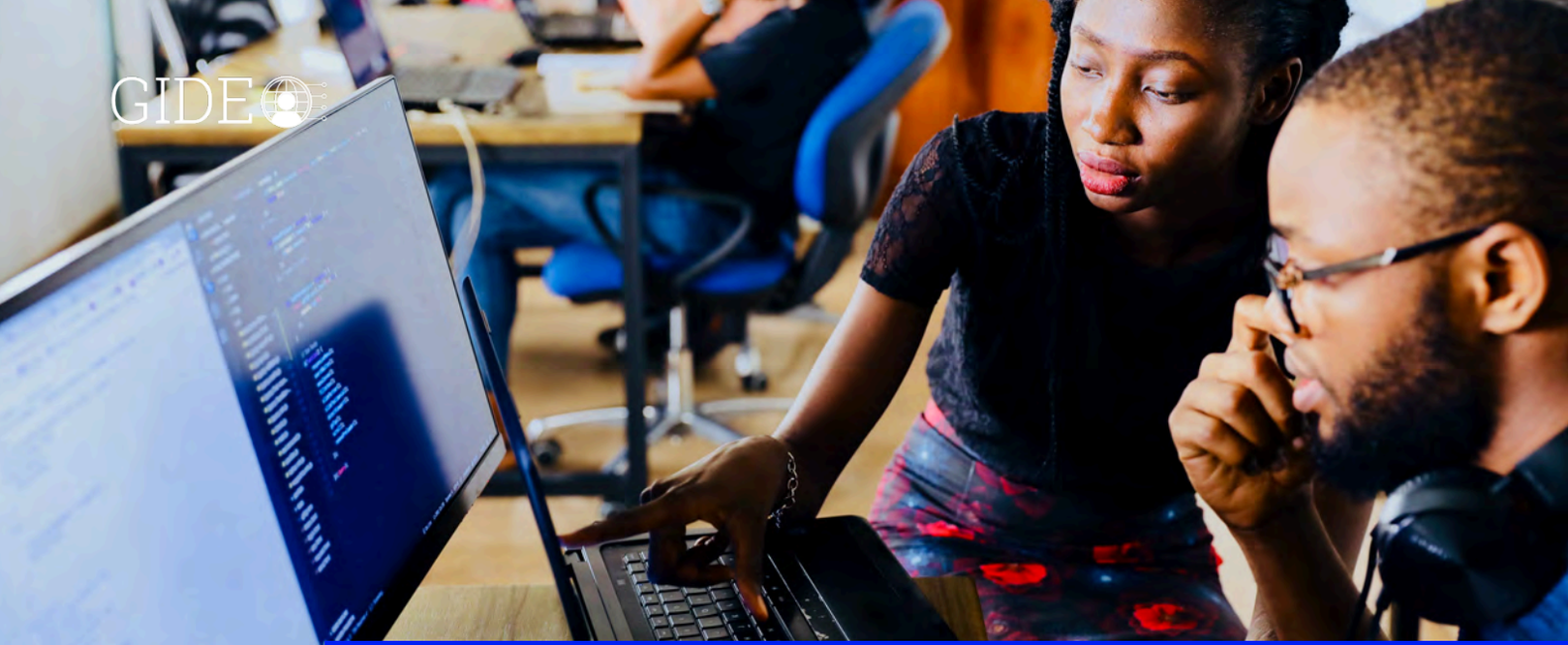
Fifth, the proposals would eliminate the current system of “third-party-financed digital barter” and thereby prevent undermining of the free market system in the allocation and distribution of resources. Thereby the proposals would provide new avenues for ensuring consumer protection, implementing a 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 have 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.

Seventh, the application of these principles to the collection and utilisation of machine learning datasets will improve the integrity and ethical deployment of Artificial Intelligence.

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.





References

Acemoglu, D., Makhdoumi, A., Malekian, A. & Ozdaglar, A. (2019). Too Much Data: Prices and Inefficiencies in Data Markets. *NBER* Working Paper No. 26296, https://www.nber.org/papers/w26296

Akerlof, G. (1970). “The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*. 84(3), 488-500.

Ali, S.N., Chen-Zion, A. & Lillethun, E. (2020). Reselling Information. *Computer Science and Game Theory*. https://arxiv.org/abs/2004.01788v1

Allen, C. (2016). The Path to Self-Sovereign Identities. [Blog post] retrieved from www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Apple, (2020). Apple and Google partner on COVID 19 contact tracing technology. [Newsroom post] retrieved from /www.apple.com/au/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Arrieta-Ibarra, I., Goff, L., Jiménez-Hernández, D., Lanier, J. & Glen Weyl, E. (2018). Should We Treat Data as Labor? Moving Beyond ‘Free’. *American Economic Review, Papers and Proceedings*. 108, 38-42.

Atkinson, J. W., & Feather., N. T. (1966). *A Theory of Achievement Motivation*. New York: Wiley.

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

Baumeister, R. F., Bratslavsky, E., Finkenauer, C. & Vohs, K. D. (2001). Bad is Stronger than Good. *Review of General Psychology*. 5(4), 323-370 https://journals.sagepub.com/doi/abs/10.1037/1089-2680.5.4.323.

Blankertz, A. (2020). Designing Data Trusts; Why We Need to Test Consumer Data Trusts Now. *Stiftung Neue Verantwortung*. 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, I. (2016). The Economics of Privacy, Data Protection and Surveillance. *In Handbook on the Economics of the Internet*, ed. J.M. Bauer & 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, J. M. (1965). An Economic Theory of Clubs. *Economica*, New Series. 32(125) 1-14.

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

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

Cornes, R. & Sandler, T. (1996). *The Theory of Externalities, Public Goods and Club Goods*. Cambridge University Press, 2nd ed.

Criado Perez, C. (2019). *Invisible Women: Exposing Data Bias in a World Designed for Men*. London: Chatto & Windus.

Delacroix, S. & Lawrence, N. (2018). Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. *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, L. (2020). *The Internet in Everything*. New Haven: Yale University Press

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

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

Edwards, L. (2004). The Problem with Privacy. *International Review of Law Computers & Technology*. 18(3), 263-294 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1857536

Englehardt, S. & Narayanan, A. (2016). Online Tracking: A 1-Million-Site Measurement and Analysis. http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

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

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

Fairfield, J. (2017) *Property, Privacy and the New Digital Serfdom*. Cambridge: Cambridge University Press.

Farboodi, M., Mihet, R., Philippon, T. & Veldkamp, L. (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

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, M. & Paal, B. (2019). *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., Surico, P. & Steiner, J. (2020). The Value of Testing. VoxEU.org, 23 April. https://voxeu.org/article/value-testing

Gazzaley, A. & Rosen, L. (2016). *The Distracted Mind: Ancient Brains in a High-Tech World*. Cambridge, Mass: MIT Press.

Grossman, R. L., Heath, A., Murphy, M., Patterson, M. & Wells, W. (2016). A Case for Data Commons. *Computer Science Engineering*., 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, J. (2020). 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, J. (2016). *The Secret of Our Success*. Princeton: Princeton University Press.

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

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

Joskow, P. L. (2007). Regulation of Natural Monopolies. In A. M. Polinsky & S. Shavell (eds), *Handbook of Law and Economics*, vol. 2, pp 1227-1348, Elsevier. https://economics.mit.edu/files/1180

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

Kaeseburg, T. (2019). Promoting Competition in Platform Ecosystems. Vox EU.org https://voxeu.org/article/promoting-competition-platform-ecosystems

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

Kyvik Nordås, H., Lodefalk, M. & Wernberg, J. (2021). The EU Digital Market Regulations: Rule-Maker or Deal-Breaker. TIISA Policy Brief, December 2021. At https://www.diva-portal.org/smash/get/diva2:1624226/FULLTEXT01.pdf

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

Libert, T. (2015). Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites. *International Journal of Communication*. October 2015

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

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K & Dhingra, D. (2016). *Digital Globalization: the New Era of Global Flows*. McKinsey Global Institute

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

McDonald, S. & Pocaro, K. (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, W. (2018). The Duty of Data Security. *Minnesota Law Review*. 103, 1135.

Mesnard, A. & Seabright, P. (2020). Easing Lockdown – Digital Applications Can Help. VoxEU.org, 1 May https://voxeu.org/article/easing-lockdown-digital-applications-can-help

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

Morrison, S. (2021). Combatting online trolls and strengthening defamation laws. Media Release, 28 November 2021. Prime Minister, The Hon. Scott Morrison MP, Attorney-General, Senator the Hon. Michaela Cash. https://www.attorneygeneral.gov.au/media/media-releases/combatting-online-trolls-and-strengthening-defamation-laws-28-november-2021

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

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

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

Oinas-Kukkonen, H. & Harjumaa, M. (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'Regan, C. & Theil, S. (2020). Hate speech regulation on social media: An intractable contemporary challenge. *Research Outreach*, https://researchoutreach.org/wp-content/uploads/2020/02/Catherine-O-Regan.pdf

O'Shea, L. (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* ed. O. Schultheiss & J. Brunstein, 30–71. Oxford: Oxford University Press.

Poikola, A. Kuikkaniemi, K. & Honko, H. 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. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf

Posner, E. A. & Weyl, G. (2018). *Radical Markets: Uprooting Capitalism 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.

Puranic, H., Koopman, J. & Vough, H. C. (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. & Nass, C. (1996). The Media Equation: *How people treat computers, television and the new media like real people and places*. Cambridge, UK: Cambridge University Press.

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

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

Sanfilippo, M., Frischman, B. & Standburg, K. (2018). Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework. *Journal of Information Policy*. 8, 116-166, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3546349

Savelyev, A. (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, L. H. (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, T. 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, D., Roessler, B. & Nissenbaum, H. (2019). Technology, Autonomy, and Manipulation. *Internet Policy Review* 8(2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3420747

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

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

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

UNCTAD (2019), *Digital Economy Report 2019, value-creation and capture: implications for developing countries,* New York: United Nations

UNCTAD (2021), *Digital Economy Report 2021, cross-border data flows and development: For whom the data flows*, New York: United Nations

Vaishya, R., Javaid, M., Kahn, I. H. & Haleem, A. (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, L. & Chung, C. (2019). Data and the aggregate Economy. mimeo, https://www0.gsb.columbia.edu/faculty/lveldkamp/papers/JEL_MacroDataLV_v7.pdf

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

Weinberger, J., Cotler, T. & Fishman, D. (2010). The Duality of Affiliative Motivation. in *Implicit Motives* eds O. Schultheiss & J. Brunstein. Oxford: Oxford University Press

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

Wong, J., & Henderson, T. (2019). The Right to Data Portability in Practice. *International Data Privacy Law*, doi 10.1093/idpl/ipz008

Woodcock, J. & Graham, M. (2019). *The Gig Economy: A Critical Introduction*. Cambridge: Polity.

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

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

GIDE
Global Initiative for Digital Empowerment

GLOBAL SOLUTIONS
THE WORLD POLICY FORUM

THE NEW INSTITUTE