Task Force 4
**Digital Transformation**

**Policy brief**

# IMPLEMENTING HUMANISTIC DIGITAL GOVERNANCE

SEPTEMBER 2021

**Dennis J. Snower** Global Solutions Initiative Foundation
**Paul Twomey** Global Solutions Initiative Foundation

T20 NATIONAL COORDINATOR AND CHAIR
ISPI

T20 CO-CHAIR
IAI

T20 SUMMIT CO-CHAIR
Università Bocconi MILANO

THINK20 ITALY 2021

G20 ITALIA 2021

# ABSTRACT

We identify an important feature of current digital governance systems: “third-party funded digital barter” between digital consumers and third-party funders. The interests of the third-party funders are not well-aligned with the interests of the digital consumers. This fundamental flaw of current digital governance systems is responsible for an array of serious problems, including inequities, inefficiencies, manipulation of digital consumers, as well as dangers to social cohesion and democracy. We present four policy guidelines that aim to correct this flaw by shifting control of personal data from the data aggregators and their third-party funders to the digital consumers.

# CHALLENGE

The policy proposal addresses the following challenges:

User consent for what is effectively ubiquitous commercial surveillance is inadequate, given power and information asymmetries between individuals and dominant technology platforms, and the paucity of service available to those who 'opt out' means it is not a viable option for most. Data protection as currently defined and enforced is unable to secure user control of data, or freedom from commercial and even political and social manipulation.

The current market structure under-values the personal data that users must supply in order to receive most digital services, making individual control of personal data impossible. Personal data is vulnerable to cybersecurity threats, particularly those directed at the opaque networks of third parties with no relationship to the individuals whose data they exploit.

Although the digital revolution has unleashed a tidal wave of new opportunities, there is a misalignment of interests between the users of digital services (on the one hand) and the digital service providers and the third-party funders of digital services (on the other). An important feature of current digital governance systems is "third-party funded digital barter": consumers of digital services get many digital services for free (or under- priced) and in return have their personal information collected for free. In addition, the digital consumers receive advertising and other forms of influence from the third parties that fund the digital services.

The control of the planetary-scale advertising platforms that fund many Internet services is based around large quantities of personal data, much of it collected by data brokers with whom the consumer has no contractual or other relationship, which may be used to manipulate users' preferences to influence purchasing, voting, and many other behaviours (Zuboff 2019).

The misalignment between the digital consumers and the digital third-party funders is responsible for a wide variety of malfunctions, which ultimately threaten the continued functioning of our economic market systems; diminish the tax base; 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.

The benefits from the digital revolution are not immutably tied to the current digital governance regimes. The central challenge of digital governance regimes lies in finding ways of making these regimes humanistic without sacrificing the technological benefits.

# PROPOSAL

In response to these challenges, we propose the following policy guidelines:

## CONTROL OVER OFFICIAL DATA

"Official Data" (O-Data) is any data that requires authentication by the state or legally accepted sources (Generally Trusted Sources) for specified legal transactions. Examples include a user's name, date of birth, social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, credit card number, email addresses, personal telephone numbers, biometric data (retina scans, voice signatures, or facial geometry), information identifying personally owned property, and asset information.

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

The legal framework should make 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. While the content of O-Data is not controlled by data subjects (since this data requires authentication by legitimate sources), data subjects are to control and manage it.

Providing direct, effective control of first-party private data calls for mainstream use of new technological and institutional mechanisms for managing personal data, whereby the control of this data is handed from the digital service providers to the data subjects.

## CONTROL OVER P-DATA

Private Data (P-Data) is personal data that is not collective and does not require authentication. There are two kinds; "first-party P-Data" volunteered or generated by people (e.g. photos or location data from phones). "Second-party P-Data" is generated or inferred by others from existing data, e.g. profiles of people.

The data subject is to be the only legal source of first-party P-Data. Individuals are to be given genuine control over use of their first-party P-Data.

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 imple-

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

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

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

## CONTROL OVER COLLECTIVE DATA

"Collective data" (C-Data) are data that people agree to share within a well-defined group, for collective purposes that can be defined by voluntary agreements or through law.

We propose creating 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. Like a commons in the offline world – for example, an agricultural or fishing commons – the data commons has clear boundaries, roles, obligations and responsibilities that are developed and used to ensure the medium and long-term collective interests of the community that depends on these resources.

C-Data are to be under the control of effective, trustworthy and competitive organisations that promote the benefits of data subjects and the broader society.

Legislative support is required to create minimum legal definitions, protections and obligations for a range of data commons to be created. Drawing on existing types of organisations

including clubs, cooperatives, trade unions and trade associations, legal guidance or definitions will encourage the emergence of data commons that identify and meet currently unmet demand for data-sharing that protects and extends the interests of data-subjects. Legislation may also be needed to ensure data commons identify and carry out the data-sharing policies of subjects and ensure appropriate privacy and security standards are met.

The legal system is to 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. Transparency and accountability in the use of second-party P-data and C-data online should be analogous to that used offline.

## *ADDRESSING DIGITAL POWER ASYMMETRIES*

The recommendations above lay the groundwork for *providing effective rights of association for digital users*.

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 the citizens. This ensures that they are aware of who is collecting data on them and to set directly, or through an agent or collective bargaining, the terms on which they allow such data to be collected and used – including the right to refuse such collection.

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.

Data commons are a means for communities of interest to responsively manage their data – including smart-city residents, trade union and trade association members, agriculture and aquaculture cooperatives, cooperative banks – in ways that extend association to people and organisations not currently directly involved.

*Effective legal protection is to be provided for vulnerable digital users*.

Government can extend the existing regulatory requirements to act in the best interests of the data subject that apply to religious leaders, doctors, teachers, lawyers, government agencies, and others who collect and act on individuals' intimate data to also apply to data aggregators.

*Competition in the online world is to be analogous to that in the offline world*.

*Provide GAAP-like oversight is to be provided to data traffickers with regard to the protecting the data they hold*. Governments can establish a governance structure along the lines of GAAP (Generally Accepted Accounting Principles) to regulate data traffickers and ad networks to ensure individualised data are not used to manipulate.

## *IMPLEMENTATION*

This new regime will need support via institutionalisation and government policy in order to provide a level playing field for business and consumers. At the EU level, only minor legal changes are called for and the new regime can play a central role securing the European digital single market, but is fully consistent with the GDPR. Outside the EU, the new regime can play a major role in overcoming inefficiencies and inequities of the current digital governance regimes.

The next steps towards implementation include the following:

- Enable individuals to gain control over their O- and P-Data and enable social groups to gain control over their C-Data by using institution-building strategies, and a range of building on some of the lessons of Personal Information Management Systems (PIMS), self-sovereign identity (SSI) and high scale data record query and resolution.
- Address digital power asymmetries by extending competition law as well as laws to safeguard the right of association and protections for vulnerable groups.
- Enable social groups to gain control over their C-Data through the establishment and support of data-trusts, particularly data commons, using current projects to determine which additional legal and institutional supports are needed.

## *IMPLICATIONS*

This proposal has far-reaching implications:

**Consumer protection** – addresses opaque and asymmetrical data collection and exploitation, including in non-contractual relationships; creates greater ability for true data portability and interoperability – increasing competition and effective markets and creating opportunity for challenger firms – and directly addresses the use of data for commercial and political manipulation.

**Containment of Pandemics** – this proposal materially addresses the trust and coordination issues that hamper data collection, sharing and use to address COVID-19 and other public health emergencies, and the ongoing under-provision of public goods in the form of health data.

**Taxation of Digital Goods and Services** – addresses challenges of Base Erosion and Profit Shifting (BEPS) that are exacerbated through the digital economy and generates new sources of tax revenue, arising from the new informational markets that the proposals above create.

**Fundamental Rights** – protects and upholds fundamental human rights that are threatened by the current model, in particular, rights to dignity, freedom, equality, solidarity, citizens' rights and justice.

Our proposals aim to mitigate these problems while retaining the wide-ranging benefits of the current digital system. There are various channels whereby the proposals aim to achieve these ends.

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

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

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

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

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

Sixth, by giving individuals control over O- and P-Data and giving the relevant groups control over C-Data, the digital regimes would become far less vulnerable to political, social and economic manipulation. Clearly, if users 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,[1] then the users will not exploit their own psychological weaknesses and other agents will not be in a position to do so either.

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

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

# NOTES

[1] See Ostrom (1990) and Wilson, Ostrom and Cox (2014). The connection between Ostrom's management of the commons and data trusts is clarified in Wyle and McDonald (2018).

# REFERENCES


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

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

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

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

# ABOUT THE AUTHORS

**Dennis J. Snower** Global Solutions Initiative Foundation, Berlin (Germany)

Dennis J. Snower is founder and President of the Global Solutions Initiative; Professor of Macroeconomics and Sustainability at the Hertie School, Berlin; Fellow at The New Institute, Hamburg; Senior Research Fellow at the Blavatnik School of Government, Oxford; Non-resident Fellow of Brookings Institution and Visiting Professor at University College London. He was formerly President of the Kiel Institute for the World Economy.

**Paul Twomey** Global Solutions Initiative Foundation, Berlin (Germany)

Paul Twomey is a successful Chief executive and entrepreneur in cyber security and legal publishing. He is a founding figure and former CEO of ICANN. He is a Fellow of the Global Solutions Initiative and Distinguished Fellow with the Centre for International Governance Innovation.