T20 INDONESIA 2022 THINK

Policy Brief

IMPLEMENTING AN INDIVIDUAL-EMPOWERED DATA GOVERNANCE REGIME

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Paul D. Twomey, Fellow and Core Theme Leader, Global Solutions Initiative; Co-Lead of Global Initiative for Digital Empowerment, THE NEW INSTITUTE

Dennis J. Snower, President, Global Solutions Initiative Programme Director, THE NEW INSTITUTE

Abstract

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 suppliers of digital services. This policy brief identifies a central flaw of the current digital governance systems: the “third-party funded digital barter”. Consumers of digital services get many digital services for free (or under-priced) and in return have personal information about themselves collected for free. In addition, digital consumers receive advertising and other forms of influence from third parties that fund the digital services. The misalignment between 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, weaken mental health, expose users to far-ranging manipulation of attention, thought, feeling and behavior; eroding appreciation for objective notions of truth, undermining our democratic processes, and degrading 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 human-centered without sacrificing technological benefits. The policy brief presents four policy guidelines that aim to correct this flaw by shifting control of personal data from the data aggregators and their third-party funders to the digital consumers. The proposals cover “official data” that requires official authentication, “privy data” that is either generated by the data subjects about themselves or by second parties, and “collective data.” The proposals put each of these data types under the individual or collective control of the data subjects. There are also proposals to mitigate asymmetries of information and market power. The policy brief outlines in detail the technical mechanisms and business models which will enable the proposals to be practically implemented in a very large scale.

Challenges

Although the digital revolution has unleashed new opportunities for economic, social and political exchange, there is a misalignment of interests between users and suppliers of digital services. Building on unprecedented network effects, and consequent rewards to first movers (especially those offering "free" services to maximize market penetration), many digital service providers have business models built on massive user surveillance and data aggregation. This has fueled a market of more than USD 465 billion between data aggregators and entities seeking to influence users (Statista 2021). 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 variety of malfunctions, which threaten the functioning of our economic market systems; expose consumers, businesses and governments to cybersecurity threats; expose users to manipulation of attention and behavior; erode appreciation for objective notions of truth, undermine democratic processes; weaken mental health; threaten human rights and degrade social cohesion.

While governments have sought to respond through a consumer protection approach, they have failed to introduce market forces to the relationship between the individuals, digital service providers, and third-party funders. Furthermore, the application of a "one size fits all" definition of personal data has failed to keep up with how data collection has been expanded and changed though technological change.

Proposals for G20

This policy brief proposes ways in which G20 governments can achieve an active market role for citizens, shifting the regulatory paradigm towards an individual-empowered, human-centered data governance regime. In short, this could be achieved by:

- Adopting a multi-tiered definition for personal information with different policy requirements for each tier. We propose three types of personal data (Snower & Twomey, 2022):
    - **O-Data** ("Official Data") is the sort of data normally required for entering a contract or satisfying government or major institution identity requirements. O-Data is controlled by the data subject, but authenticated by trusted third parties.
    - **P-Data** is "privy data" related to individuals which is not collective and does not require authentication by third parties. This data may be divided into "first-party data" (such as photographs) generated by the data subject, and "second-party data" generated by a second party (such as location data from smartphones or past purchase records) 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 for well-defined collective purposes.
- Ensuring that long standing rules in the offline economy to protect the vulnerable from manipulation by those holding data on them (*e.g.,* doctor-patient) also apply online. The offline test is that such data should be used in the best interests of the data subject.
- Applying the lessons from existing large scale, data management systems to improve the cybersecurity around individuals' O-Data and reduce fraud to business, citizens, and government.

On this basis, we propose the following four policy guidelines:

- **Proposals 1: Control over O-Data**
    - Proposal 1a: O-Data must receive official (Generally Trusted Source) authentication and this is to be the only legal source of this data.
    - Proposal 1b: Give individuals genuine control over the use of their O-Data through easy-to-use technical tools and supporting institutions.
- **Proposals 2: Control over P-Data**
    - Proposal 2a: The data subject is to be the only legal source of first-party P-Data.
    - Proposal 2b: Give individuals genuine control over the use of their first-party P-Data, through the above-mentioned technical tools and supporting institutions.

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

- **Proposals 3: Control over C-Data**
  - Proposal 3a: Create legal structures to support the establishment of "data commons" for C-Data.
  - Proposal 3b: Ensure that C-Data is under the control of effective, trustworthy and competitive organizations that promote the benefits of data subjects and the broader society.
  - 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, are transparent and accountable.

- **Proposals 4: Addressing Digital Power Asymmetries**
  - Proposal 4a: Provide effective rights of association for digital users.
  - Proposal 4b: Provide effective legal protection for vulnerable digital users.
  - Proposal 4c: Ensure that competition in the online world is analogous to that in the offline world.
  - Proposal 4d: Provide GAAP-like oversight to data traffickers with regard to protecting the data they hold.

We propose models for how the data could be securely held and accessed and also possible business ecosystems which would build non-existing technologies (Snower & Twomey, 2022).

These proposals have far-reaching implications:

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

Containment of Pandemics – these proposals materially address 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 – address challenges of Base Erosion and Profit Shifting (BEPS) that are exacerbated through the digital economy and generate new sources of tax revenue arising from the new informational markets that the proposals above create.

Fundamental Rights – protect and uphold fundamental human rights that are threatened by the current model, in particular, rights to dignity, freedom, equality, solidarity, and 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.

- Giving individuals control over their O-Data 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).
- Individual control over O-Data and P-Data also permits addressing digital power asymmetries analogously to those in the offline world, thereby mitigating existing inequities.
- Individual control over O-Data and P-Data, along with support for the establishment of data commons, would significantly enhance the enforcement of data protection rights.
- The use of O-Data and associated use of P-Data and C-Data would significantly reduce a wide variety of cybersecurity threats.
- 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. 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.
- By giving individuals control over O-Data 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 Elinor Ostrom's Core Design Principles (Ostrom, 1990; Wilson, Ostrom and Cox, 2014), 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—as opposed to third-party funders—drive the ongoing development of digital services.

Implementations

This new regime will need support via institutionalization and government policy in order to provide a level playing field for businesses and consumers. At the EU level, only some legal changes are called for and the new regime can play a central role securing the European digital single market while remaining fully consistent with the GDPR. Outside the EU, within most of the G20 countries, the new regime can contribute significantly to overcoming inefficiencies and inequities in the current digital governance regimes. The new regime can play a major role and will contribute to the G20 presidency priorities of Digital Transformation.

The next steps towards implementation include the following:

- Enable individuals to gain control over their O-Data 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 rights to 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.

References

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

Snower, D.J., & Twomey, P. D. (2022, March 28). *Empowering digital citizens. Making humane markets work in the digital age*. Global Initiative for Digital Empowerment. Retrieved April 26, 2022, from https://thegide.org/digital-citizens-report

Statista (2022). *Worldwide digital advertising in 2021*. Statista. Retrieved April 26, 2022, from https://www.statista.com/outlook/dmo/digital-advertising/worldwide#global-comparison

Wilson, D. S., Ostrom, E., & Cox, M. E. (2013). Generalizing the core design principles for the efficacy of groups. *Journal of Economic Behavior & Organization*, 90, S21-S32.

Wylie, B., & McDonald, S. M. (2018, October 9). *What is a data trust?* Centre for International Governance Innovation. Retreived April 26, 2022, from: https://www.cigionline.org/articles/what-data-trust/

About the authors

Dennis J. Snower - Global Solutions Initiative; THE NEW INSTITUTE

Dennis J. Snower is Professor of Macroeconomics and Sustainability at the Hertie School in Berlin, the President of the Global Solutions Initiative, Program Director at THE NEW INSTITUTE and co-lead of the “Global Initiative for Digital Empowerment”, Senior Research Fellow at the Blavatnik School of Government in Oxford University, and a Non-Resident Senior Fellow at the Brookings Institution in Washington, D.C. He is an expert on labor economics and public policy and is well-known for the insider-outsider theory of employment and unemployment which he developed together with Assar Lindbeck. Dennis has acted as an adviser to a variety of international organizations and national governments and has published extensively on employment policy, the design of social systems, caring economics, and monetary and fiscal policy.

Paul D. Twomey – Global Solutions Initiative; THE NEW INSTITUTE

Paul is a serial entrepreneur in the legal, cybersecurity, talent and biosecurity sectors. Paul is a Fellow and Core Theme Leader for “managing information and technology in the public interest” at the Global Solutions Initiative and is the co-lead of the “Global Initiative for Digital Empowerment” at THE NEW INSTITUTE. He is also a distinguished fellow at the Center for International Governance Innovation and a Commissioner of the Global Commission for Internet Governance. Paul is a founding figure and former CEO of ICANN, the global coordination body of the Internet, a role in which he was described by the New York Times as "The Chief Operating Officer of the Internet". Paul was CEO of the Australian Government's National Office for the Information Economy and Deputy at the Australian Trade Commission. Formerly with McKinsey& Company, he was a special advisor to several Australian Ministers in the Keating and Howard Governments. He is a member of the SAP Artificial Intelligence Ethics Advisory Panel. He received his PhD from Cambridge University.