# A HUMAN-CENTRED DIGITAL FUTURE

**PAUL TWOMEY** of the Global Initiative for Digital Empowerment argues that consumers need to be a central part of the 'market for data'

Recent advances in artificial intelligence have only served to accentuate the need for consumers to have control over how and when data about them is processed and used, and in what circumstances. At the Global Initiative for Digital Empowerment (GIDE), we believe that there is a fundamental imbalance of power in digital markets, that this is creating a range of both societal and economic problems, and that the best way to resolve these is to make consumers active economic participants. In this respect, our proposal builds on many of the ideas within the EU's new Digital Markets Act and Digital Services Act, and in the General Data Protection Regulation.

## PROBLEMS WITH DATA GOVERNANCE

The current regime for data governance has enabled all kinds of problems to proliferate on the internet. From inadequate privacy protection to misinformation, manipulation and hate speech, it is becoming increasingly clear that the great benefits of the digital transformation are being undermined by damage inflicted on social cohesion, market economies and democracy itself. Small wonder that a global survey of over 14,000 citizens in 20 countries shows a strong majority of respondents agreeing that new government policies are required to improve trust on the internet.[1]

While the problems are many, we believe the cause can be traced to a single and fundamental point of origin: third-party digital barter, leading to a misalignment of interests between digital consumers and third-party actors. It's worth considering this in more detail.

## WHY IT'S NOT A FUNCTIONING MARKET

A traditional economic model involves the exchange between consumer and provider in which revenue flows to the latter from the former, with products and services travelling the other way. This could be described as 'visible trade' and online is best evidenced by e-commerce. However, the other 'revenue' of digital service providers is mainly in the form of the personal information extracted by them to an extent almost no consumer understands. This is a digital barter, or 'invisible trade', in which the service provider effectively bundles personal information and sells it to other producers and influencers. While the exchange between providers and other influence actors, such as advertisers, acts as a market, the invisible trade in extracting personal data does not, because the consumer is effectively excluded from the understanding and from ant decision making.

The current policy approach is to deal with the symptoms in isolation through a combination of privacy policy, competition law, consumer rights legislation, taxation and voluntary guidelines. However, this results only in policymakers engaging in a never-ending battle against systemically inappropriate incentives. We argue that a much better solution is to make consumers active market participants by giving them control of their personal data, individually and collectively. They should be able to approve who has access to their personal data and on what terms, giving them a point of leverage and rights of association. In return, individuals would be required to maintain accurate, authenticated data.

## PERSONAL DATA

The data normally required for entering a contract or satisfying the identity requirements of government or major institutions is 'personal data', such as that defined in the EU's General Data Protection Regulation. Examples include names, addresses, personal identification numbers, personal characteristics such as biometric data and personal asset information like MAC addresses.

Personal data should be maintained by citizens in a trusted repository and they should have the obligation to ensure that the data is authenticated by legally accepted sources. Just as data on a passport or identity card held by an individual is legally required to check in to a European hotel, the repository should be the sole initial legal source of this data for public and private transactions, unless specifically stated otherwise by law. The data accessed by an entity could carry a transaction-specific digital signature confirming that the data in the hands of the entity has been sourced correctly. These data holdings would be open to audit.

An extension of personal data is that related to individuals, but which is not collective and does not require authentication by third parties. It includes 'first party' data, such as blogs and personal photographs which are generated by the data subject

and 'second party' data, generated by a second party about the data subject, such as location data from smartphones or records of a person's past purchases. This includes AI inferences and passive data obtained autonomously.

First party data is placed online by the user in the context of a contractual or other legal relationship with a company such as a cloud operator, telco, app provider or employer. This legal relationship will require the company also to link to or hold the individual's personal data and negotiated preferences as part of their account management processes. Use of this data should be negotiated on behalf of citizens by data market professionals, who would advise on what terms should apply to the use of their personal data. Citizens would be provided with effective rights of association and representation.

Second-party data is inferred about the data subject and just as in existing offline rules (like doctor-patient standards), such data is to be used only in the interests of that subject. Legal protections can be drawn from 'fiduciary law' frameworks.

## DATA COMMONS

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. This would include, for example, medical databases and location data for traffic management. The data commons is a defined and protected structure to which people can delegate the stewardship of certain subsets of their personal data. 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 meet currently unmet demand for data sharing that protects and extends the interests of data subjects. We propose that:

- Legal structures are created to support the establishment of 'data commons'.
- Common data are under the control of effective, trustworthy and competitive organisations that promote the benefits of data subjects and the broader society.
- The data commons are permitted to use data only for specified purposes and its use is transparent and accountable.

The proposed representative/agent role to support consumers will also be an effective mechanism for determining if consumers are interested in participating in data commons initiatives.

## ADDRESSING DIGITAL POWER

In order to address the asymmetries of digital power our proposals include the provision of effective rights of association (enabling consumers to act in their own best interest) and legal protection for vulnerable users. It's important that competition in the online world is in every respect analogous to that in the offline world. Data should be cryptographically hashed specific to each entity and consumer records subject to oversight through GAAP-style standards[2], enforced through audits. This ensures that entities collecting personal

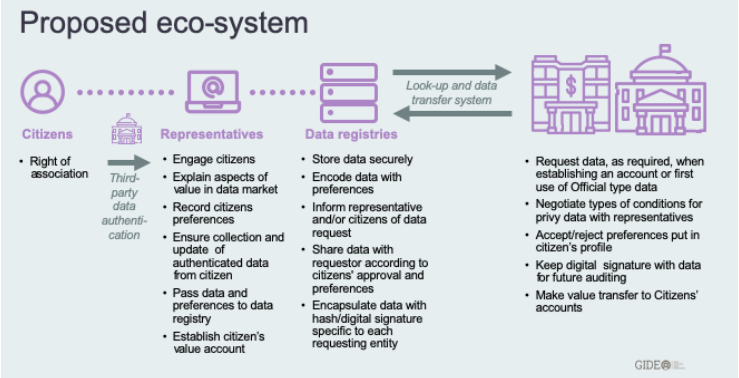
### KEY PRINCIPLES FOR RELINKING SOCIAL WELL-BEING WITH ECONOMIC BENEFITS IN THE DIGITAL SOCIETY

- Bring all users into the market and empower them as market participants: to approve who accesses their data and on what terms
- Give individuals a point of leverage and rights of association so that they can access data market skills
- In return, require individuals to maintain accurate, authenticated data
- Adopt a multi-tiered definition for personal information with different policy requirements for each tier
- Build on existing technology and business models like the Domain Name System or credit card processing system
- Apply long standing rules in the offline economy to protect the vulnerable from manipulation (e.g. doctor-patient) to online actors
- Improve the cybersecurity around individuals' personal data and reduce fraud in business, for citizens and in government.
- Enable and incentivise data commons for the public good

information, especially those involved in data trafficking, abide by the rules to source personal data only from the consumer-controlled repository. Audits would ensure that entities use personal data from the prescribed source and provide a third party to verify that those holding intimate user data act in a way that is transparent to consumers and is in the individuals' interests.

## BUILDING ON EXISTING RULES

The policy thrust of the EU's General Data Protection Regulation, the Digital Services Act, Digital Markets Act and Data Governance Act all represent steps in the right direction towards the principles we are advocating. However, they fall short of affording individuals full transparency and control over who has information on them, nor do they establish the long term benefits of integrating consumers as economic actors in the digital data market. By treating personal data as a means of production and giving citizens control over it, our proposals redraw the relationship between markets, companies and consumers.




## A PROPOSED ECO-SYSTEM

The system proposed by the Global Initiative for Digital Empowerment envisages four principal actors:

- **Citizens**, armed with the right of association.
- **Representatives** will record citizens' preferences, and collect and update their personal data before passing it on to a data registry. They will also establish a citizen's 'value account'.
- **Data registries** securely store the data, encoded with preferences. They share data with requestors according to those preferences, informing representatives and/or citizens. They encapsulate data with a digital signature specific to each requesting entity.
- **Requestors**: companies and organisations making use of personal data, establish an account for use of personal data and negotiate conditions for the use of first and second party data with representatives. They keep a digital signature for future auditing and make value transfers to citizens' accounts.

Multiple technologies exist to support these data flows. Examples include high speed database and resolution systems such as the Domain Name System, hybrid blockchain storage such as Seal and personal ID wallets such as the European Digital Identity (eID) system currently under trial. Policymakers do not need to pick a technology, but rather encourage an industry standard or promote competition with interoperability. Governance would be supported by a system of security, commercial and stability audits, in many cases building on existing audit regimes.

## SUMMARY

Human-centred digital governance empowers individuals and market forces to enable many of the privacy, consumer protection, and transparency concerns to be negotiated in a manner that keeps pace with rapid technological change. It brings tangible benefits to businesses by ensuring accurate customer information and reducing the likelihood of fraud, and will fuel innovation and new business creation. Governments still have a role in protecting their citizens through evolving privacy rights built on a foundation of consumer protection reforms. But government is slow. Rather than having to play catch-up after several electoral cycles, governments will be able to have confidence that the negotiations on behalf of citizens within the new market will resolve many of the consumer's concerns. Introducing market forces to the relationship between empowered consumers, digital service providers (those that collect the data) and third-party influencers (those who purchase and use it) will help diminish the whack-a-mole problem of having to counter mutating types of data misuse that permeates the current system.

## CURRENT STATUS

The proposals put forward by GIDE have attracted increasing interest from international policy makers. A series of ongoing detailed discussions have been held at EU organs, especially the European Commission and the European Parliament. Other developed and developing country governments have expressed interest and at least one is conducting exercises to consider the implications of introducing such a model. Recently GIDE was asked to present its proposals to member states of UNCTAD[3] and to the Think20 organ of the G20. Similarly, the World Bank has partnered with GIDE to further the Bank's GovTech initiative.[4]

*The Global Initiative for Digital Empowerment is an international group of researchers, policymakers, civil society advocates, technical experts and business people dedicated to reforming the rules for the global digital economy. For the full report, 'Empowering Digital Citizens' see thegide.org/empowering-digital-citizen-report/*

***PAUL TWOMEY*** *is Co-Chair of the GIDE and a distinguished fellow at the Centre for International Governance Innovation. He was a founding figure and former CEO of ICANN, and CEO of the Australian Government's National Office for the Information Economy.*

**REFERENCES 1** This survey was conducted in 2021-22 by Ipsos for Fen Osler Hampson, Carleton University and Visiting Fellow, The New Institute. **2** 'Generally accepted accounting principles', the accounting standard adopted by the US Securities and Exchange Commission and the default accounting standard used by companies based in the United States. **3** UN Conference on Trade and Development. **4** https://www.worldbank.org/en/programs/govtech