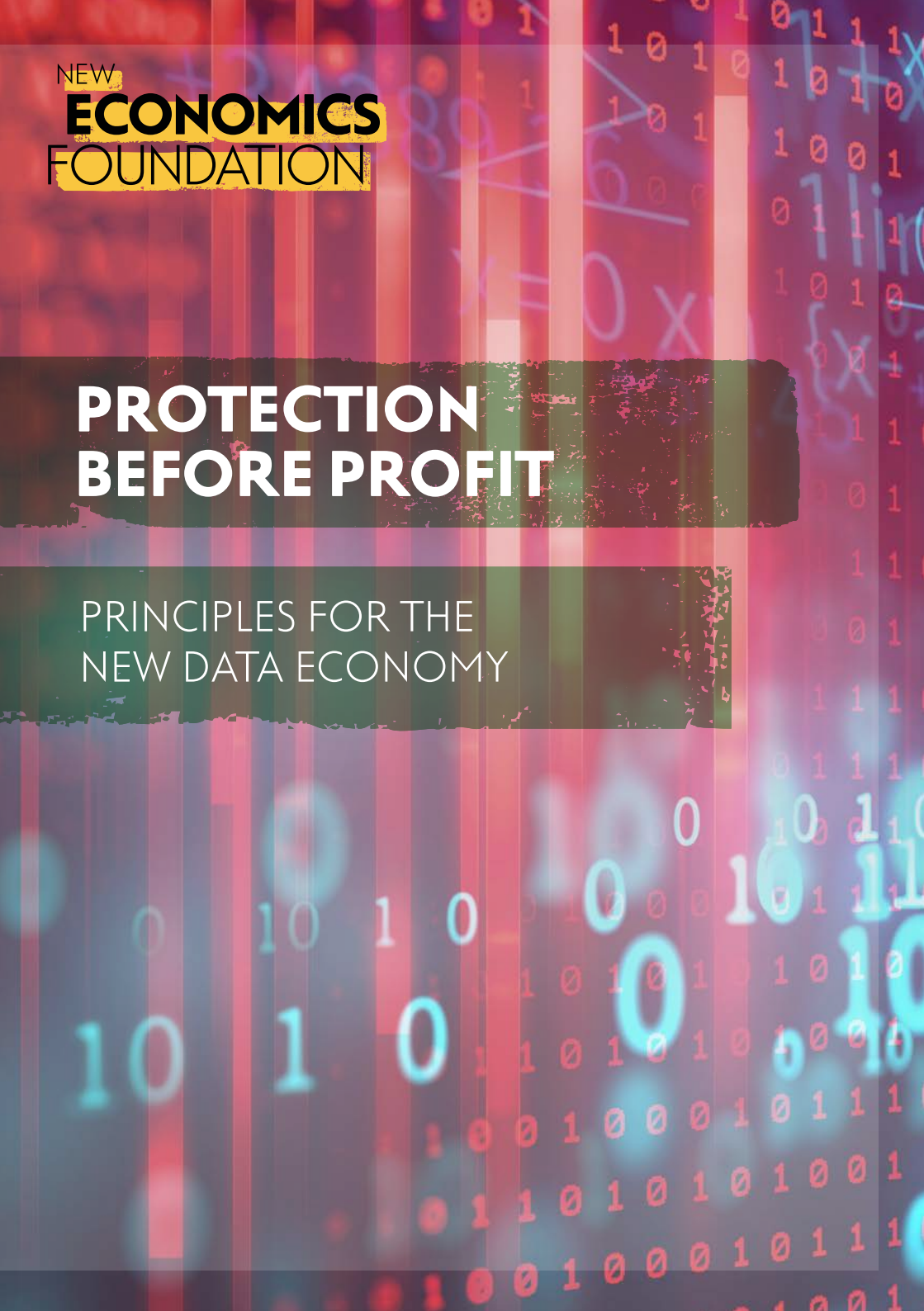
NEW ECONOMICS FOUNDATION

PROTECTION BEFORE PROFIT

PRINCIPLES FOR THE NEW DATA ECONOMY




NEW
ECONOMICS
FOUNDATION

CONTENTS

INTRODUCTION

Data sustains the modern digital economy, from online services and apps, to our favourite websites. The collection and monetisation of data has created a new business model where we get access to, and use of, a whole range of services for free in return for allowing companies to track and analyse us. From maps and translation services, to email, we enjoy these free services because the companies that provide them get something in return: our data.

The data economy is still very young, but it's already transforming our economy and society. It's evolving extremely quickly, driven by the increasing technical capabilities of hardware and software. This proliferates its economic and social impact, both positive and negative. There's a real urgency that this is taken seriously by regulators now, if we're to ensure a net positive impact as we integrate this new technology and resource into our economy. To do this we must spread the power that data creates more widely, and create new accountability mechanisms to hold data economy actors, both public and private, to account.

The Internet was initially developed to meet the needs and requirements of the US military which 'shaped the system into a powerful tool of government surveillance'.[1] But the modern data economy is now being led by private companies seeking to capture data about us for their own purposes. Many of the techniques used by these companies have become part of the everyday digital economy without the consent of the users. From having every interaction with the digital world recorded and analysed, to being served personalised adverts, personal data is being traded around the world, and is subject to constant scoring by algorithmic systems based on inaccurate profile information. Democratic accountability is absent. Instead, people, collectively, need to be put at the centre of the future data economy to ensure that it serves and protects them rather than the interests of big business and government.

Many countries still have no legislation covering the use and processing of most data, with exceptions for medical and financial data and anti-discrimination legislation. This has left the private sector free to innovate without constraint and lead this radical transformation in

the economy, ensuring its interests are being met at the expense of those of the public and society more broadly. We therefore have a data economy that's primarily focussed on meeting the needs of a small group of entrepreneurial capitalists. At the same time, these companies try to ensure that consumers still feel like they're getting something, a free service or cheap goods (even though in reality, the 'consumers' are more like products for sale to advertisers from sites like Facebook). But we must be clear. As the data economy functions today, if our rights, as people, conflict with their interests, as companies, it's the company's interests that almost always triumph.

The tide, however, is starting to shift. The EU has started to set some ground rules for the collection and processing of our personal data with the implementation of General Data Protection Regulation (GDPR). This marks a vitally important step towards governments being able to regulate and regain some control over a system in which data collection and processing has been growing out of control. However, the GDPR has not yet done much to curtail the power of the tech giants. These companies can rely on lawyers to navigate the complex legal structures of this legislation and avoid the potential restrictions it poses, in a way that small and medium enterprises (SMEs) cannot do.[2,3] Nor has the GDPR created the clear accountability or the strong protections that we hoped for, since redress is still very hard to get and certain rights, like the Right to an Explanation, have an extremely limited scope.[4]

The emerging fields of 'algorithmic accountability' or 'ethics in artificial intelligence (AI)' promoted by social scientists, lawyers, and computer scientists also have limitations. These are frequently conceived as purely technical projects involving, for example, the reduction of bias through more comprehensive data collection, rather than complex moral and political ones. But by focussing on the narrowly legalistic issues of fairness or accuracy, these approaches risk downplaying the larger moral and political implications of these technologies existing in society. As Frank Pasquale (Professor of Law at the University of Maryland and a member of the Council for Big Data, Ethics, and Society) highlights: 'By trying to make these games fairer, the research elides the possibility of rejecting them altogether.'

We must ensure that the future data economy puts the protection of people above the interests of private companies' quest for profit, or the government's desire to monitor. The stakes are too high to fail. Multiple reforms and interventions will be needed to achieve a just and equitable data economy.

Here, we set out six principles to guide this transition:

- **PROTECT BY DEFAULT**
  Hardware, software, and platforms should protect users by default and ensure people have automatically enabled new features and protections.

- **BUILD ON A DECENTRALISED ARCHITECTURE**
  Digital infrastructures should be based as far as possible on decentralised architecture to disperse power, while creating a more secure and less vulnerable network.

- **ENABLE THE COLLECTIVE**
  The narrative around individual rights and actions needs to be supplemented by a narrative around collective rights and actions. The individualised narrative is hugely disempowering because it excludes those people who do not have the time, ability, knowledge, or interest to take action to protect themselves from potential harm.

- **REALISE THAT DATA IS A PUBLIC GOOD**
  The data economy is too focussed on the monetary value of data. This is favoured at the expense of it being put towards the public and social good. Because of its ability to help us transform the economy for the common good, we must realise that the real value of data is not monetary, but social. If we fail to realise this, our data economy will always be susceptible to the whims of the private sector.

- **ENSURE CLEAR ACCOUNTABILITY**
  As the data economy enters more areas of our life, we need to ensure there is clear accountability for those collecting and processing our data.

- **INCREASE TRANSPARENCY**
  Finally, we need to ensure that there is transparency within the system. This will help rekindle trust in the data economy, so damaged by recent scandals and leaks, and hamper big tech's love of opaque business practices that characterise the digital world today, such as blanket data collection.

PROTECT BY DEFAULT

The impact of an intervention differs greatly depending on whether it establishes a new default setting rather than requires individual action. The future data economy should seek to protect us by default without requiring additional action. The clear assumption should be that we all want our rights and privacy respected. Some well-discussed interventions in this area are known as 'privacy by default' often complemented by 'privacy by design'. Privacy by default seeks to ensure that the services we use assume provide total privacy. We should seek to create systems that respect this, with additional tools and options for those who wish to go further and share data online. Privacy by design looks at how design choices impact privacy decisions and sets out to prioritise privacy over

EXAMPLE 1. AD BLOCKING.

In January 2018, Safari, Apple's graphical web browser, implemented a feature that prevented users from being tracked around the Internet through the careful management of cookies (small pieces of code that allow companies to continuously identify users as they browse). This simple intervention by a major tech company, which set a new default for all users of the browser, had a massive impact on the amount of tracking data being created, thereby somewhat reducing the digital panopticon in which we are increasingly living. The effect of the new default setting can also be seen in the adtech industry's revenue with companies like Criteo, the Paris-based personalised retargeting company, claiming they expected their revenue to drop by 20% immediately as they can no longer collect as much data on Safari users.[5] This can be contrasted with the efforts of other browsers and platforms to offer users additional control and options so that they can manage their own settings. Evidence suggests that in the UK only 22% of people apply ad blockers, demonstrating their limited reach.[6]

design. It should not be possible for designers or system architects to assume that we don't want our privacy protected. Nor should it be possible for companies to only provide tools and settings for people to change privacy settings manually and cumbersomely, in order to stop the collection and sharing of data. We shouldn't allow the interests of tech giants to triumph over the wider needs of people and society.

The setting of new defaults would make it easier to hold tech companies to account, since their overriding duty would be to protect individuals from harm, such as unauthorised data harvesting.

BUILD ON A DECENTRALISED ARCHITECTURE

Theoretically, the Internet is still decentralised in that no one owns all, or a considerable portion of, the network or infrastructure that connects the World Wide Web. Anyone can still publish content on the Web without having to rely on a specific company or service provider. Today, however, the balance of power has been skewed. Companies like Google and Facebook have worked to reshape the architecture of the Internet to increase their gatekeeping power over the information that circulates.

BOX 1. FROM A DECENTRALISED TO A CENTRALISED INTERNET

The US Department of Defense originally conceived the structure of the Internet as a decentralised architecture, so that it could withstand unforeseen events and wars.[7] In this case, decentralisation allowed the system to keep running even if one of its parts was incapacitated. The early days of the Internet were very chaotic and highly decentralised. There was no central authority. Every computer was independent. Although there were advantages, such as the fact that no one could shut off the network, there were also disadvantages. If the server holding the information you required went down, then you weren't able to retrieve it. There was also the inconvenience of having to dial a new number for every server.

As the Internet moved out of its early use phase as a tool for the military and research communities, and evolved into the commercial entity we know today, it started transitioning towards the centralised network that it has become. Gone are the days when we could access the Internet independently. For all but the most knowledgeable users, accessing the Internet now requires an Internet service provider (ISP);

millions of UK Internet users all connect through a very limited number of ISPs. The development of the Internet server client model was another important development that encouraged further centralisation. The implication of this is that all of the websites we visit are sent to us from servers rather than from computer to computer. As an example, when we visit a friend's Facebook page, this information is served from Facebook's central servers, not from our friend's computer. Centralisation is further re-enforced by the fact that a relatively small number of sites account for the majority of traffic: Netflix and YouTube now account for 25% of all Internet traffic,[8] while the top 100 websites account for the vast majority of all activity.[9]

In a highly centralised Internet, the power shifts towards the big technology companies. Because the majority of traffic now passes through their servers, they are essentially acting as ISPs and platforms, giving them the power to monitor and influence activities. Without this highly centralised architecture, the Internet would not have evolved into the form in which it exists today.

Although we have seen many benefits, there are also some serious downsides. Users are left disempowered. Access to content has left them at the mercy of the provider and the platform. All of the services and platforms we use have single points of failure, which leaves our data more vulnerable to attack and the consequences of a more severe attack. Centralised systems are also easy targets for disruptive activities. For example, Distributed Denial of Service (DDoS) attacks, which are malicious attempts to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or user with a flood of Internet traffic, service outages, and malware virus infections.[10]

A decentralised architecture would curtail the power of corporate and state interests by reducing our reliance on their large-scale systems. It will also disperse power through people and SMEs being able to contribute their IT equipment to help extend and secure the decentralised Internet.[11] Decentralised architecture is inherently more secure and would therefore help protect our information online by distributing it across many locations so that each hack yields less data.

EXAMPLE 2. MASTODON: THE DECENTRALISED TWITTER

Mastodon is a project which began in October 2016 to create a decentralised alternative to Twitter. Mastodon uses OStatus, an open protocol for decentralised microblogging used by many services. The user interface mimics the functionality of Tweetdeck, which has helped to migrate Twitter users already familiar with the layout. Although hard to estimate, there are about 1.5 million people using Mastodon at present.[12]

Mastodon has no money, shows no advertisements, and has raised no venture capital. It has no board of directors, no VP of Product, no Chief Financial Officer, and yet it is growing steadily.

It allows anyone with computer to set up an 'instance' best described as a version of the programme that is stored and managed locally.

The person initiating the instance becomes the server administrator and is responsible for setting and enforcing rules on their instance. Those rules can vary, sometimes widely, from instance to instance.[13] For example, some forbid adult content while others forbid pro-Nazi content.

To still benefit from the positive network effects associated with platforms, Mastodon has to support the ability to share messages with users of other servers. This demonstrates the power of decentralised architecture where each instance can be autonomous and in control, setting their own rules locally, while also being part of a wider network with shared rules and protocols, thus enabling them to benefit from scale and network effects.

ENABLE THE COLLECTIVE

Many interventions in the data economy, such as the GDPR, are heavily focussed on the individual, just as the dominant economic narrative, neoliberal economics, stresses the importance of individual autonomy and choice. The GDPR seeks to extend the scope of individual rights into the online data space by creating a new set of digital rights and responsibilities that companies and individuals need to abide by. However in the data economy, the focus on individual rights can actually be disempowering because the burden falls on the individual to take action or to seek remedies, which many people fail to do. We need the foundation of individual rights and powers set out in the GDPR to enable collective power; this is the only realistic way to realise those rights.

The data economy desperately needs interventions that shift towards enabling collective action, not only in the means through which meaningful consent is given, but also in regard to how data sharing is governed. For instance, collective legal action, in the guise of a class action lawsuit, is now possible under Article 8 of the GDPR. A group of UK residents is threatening to sue Facebook over the misuse of their data in the Cambridge Analytica scandal. It is estimated that 1.1 million people could join the suit if it proceeds.[14] Collective action empowers the individual through the action of the group and is a long-standing approach to dealing with the power asymmetries of the modern economy.

Placing the individual at the centre of the data economy ensures that those without the right technical knowledge, the necessary time, or the inclination to take action, have not been helped by the GDPR. In addition, the focus on individual rights sets up losing battles between individuals who are generally poorly resourced in terms of money and expertise, and the large tech giants with their deep pockets and near-limitless access to experts. This huge power imbalance means that individuals are often put off challenging companies and holding them to account for their actions. Even if they do proceed, the corporations always have an advantage in any dispute.

EXAMPLE 3. CONSENT

The decision to make the collection and sharing of data contingent on acquiring our personal consent is transformative. It should be empowering in terms of our digital rights. But in reality, it places an impossible burden on the individual. Few are inclined to read the terms and conditions or make independent judgements because it's time consuming and can be jargon heavy. If we actually read the terms and conditions in their totality to provide informed consent in the truest sense, a huge waste to the economy would occur. If everyone who installed Flash read the entire 3500-word terms and conditions, this would require 152 years of human attention, 24 hours a day, every single day.[15,16] If we extrapolate this for every other user licence agreement, we quickly condemn humanity to an eternity of digesting and agreeing to terms and conditions. Given these problems, the challenge remains how to make the process of gaining consent both meaningful and informed.

One possibility would be to **crowdsource the review of terms and conditions** to help highlight problematic conditions. When the UK Parliament published Facebook's internal company documents in late 2018, people started dissecting the documents and the associated terms to help interpret them.[17] Imagine if this process was standard for all major sites with the results made publicly available and easily digestible. Unacceptable conditions would quickly surface and collective action could be mobilised.

Another way forward could be to consider giving our **consent by proxy** through trusted individuals or groups, perhaps for a small fee.[18] Here, individuals with specific knowledge or skills would review a website's terms and be empowered to give consent on our behalf. Individuals who hold consent proxy for many Internet users could then also engage in collective bargaining on their behalf to ensure that problematic terms are changed. Different groups would then emerge with different appetites for sharing data, as well as other criteria. For example, gaining concessions, or specific niche interests which allow people to navigate the digital world, knowing that they're only signing up to goods and services whose conditions of access are acceptable to them.

REALISE THAT DATA IS A PUBLIC GOOD

Data can be a public good, for example helping local authorities to plan public transport or enabling health services to predict and mitigate disease. But currently, most data is used to aid private capital acquisition. Many voices are now calling for a better redistribution of data, rather than changing the way we conceptualise it.[19,20, 21]

A pertinent example is the debate about who should benefit from the monetisation of data. This often focusses on how the gains reaped from the exploitation of our personal data by corporations – which is then used to enable more personalised advertising – should be shared with individuals, social causes, or the public sector. Although a world where monetary gains are spread more widely is preferable to one where the gains are concentrated, it fails to ask the most important question: Is the activity in question is desirable in the first place? Potentially, in this circumstance, the greatest value to people would actually be to restrict and regulate the adtech industry, as we recommended in our report, *Blocking the Data Stalkers*.[22] Removing the incentive to gather data about us and to track our digital lives would be more beneficial to people, rather than allowing us to share the financial bounty generated by the collection and exploitation of our data. Sharing the bounty of data collection could create a perverse incentive to pursue more tracking and more personalised ads to generate more income.

Because the power of tech giants is partly based on the fact that they have gathered and analysed huge quantities of data, they have a huge incentive to keep it to themselves to build a competitive advantage. This strategy not only fails to realise the potential of data to contribute to social and public good, but it also holds back innovation. The best and most efficient way to achieve the goal of automated driving is not to have many companies individually investing in millions, or even billions of pounds worth of test driving, with each crunching that data to produce competitive products. Rather it would be much more efficient if all driving data produced by automated cars was pooled and each manufacturer was given access to it. Instead of the challenge being how good you are at generating

and enclosing data, it then becomes how good you are at processing and integrating that data into advancing technology.

Presently, health data is the most obvious type of data that is deemed to have economic value,[23] but whose value in reality should lie in the public good. Pooling our health data has the undeniable potential to allow machine learning systems to find hidden correlations and connections in the data, which could lead to a new generation of medicines and treatments.[24] There are obvious concerns, however, with sharing our most sensitive and personal data, so we desperately need to find a secure mechanism to enable this.

EXAMPLE 4. MIDATA.COOP[25]

MIDATA.coop is an exciting new initiative in Switzerland that allows people to safely store, access and share their medical data. So that people also have control of the company it is structured as a cooperative. Those within the cooperative can add a wide variety of personal and health data examples of which include hospital records and fitness trackers.

Dr Ernst Hafen, co-founder and president of the cooperative, said: 'We do not want to introduce financial incentives for data sharing because that's exactly the wrong incentive. That's what everyone does and we want to change [that].'[26]

The primary motivation for people to share their data is to help with medical research they care about. Patients within MIDATA.coop gain collective influence by pooling their data, creating a valuable resource which pharmaceutical companies can access, but only on certain terms (such as openness about the results of their research).

Any money made from this data is invested back into the community in ways decided by members of the cooperative, rather than provided as dividends to shareholders.

Though a fairly young initiative (founded in 2015), it has already seen some successes. The first pilot saw post-bariatric surgery patients recording health data, like their weight loss, and sharing it with doctors investigating the postoperative recovery period. The latest study examines a drug's effect on multiple sclerosis patients by analysing the data they input about motoric and cognitive capabilities on an app.

ENSURE CLEAR ACCOUNTABILITY

The inability to hold the powerful players in the data economy to account is a major issue. Therefore, one of the principles of the data economy should be to ensure clear accountability, which facilitates people who need further explanations about how algorithmic decisions are made about them, and which enables people to audit the system and ultimately seek redress. We have identified two different ways in which accountability should be deemed vital, but where it is currently lacking.

First, people need clearer mechanisms by which they can hold companies engaged in the data economy accountable. Secondly, they need clarity about the limits to which the data economy can hold us accountable for.

Companies and the public sector that engage in data collection and processing must understand that they are accountable for how they collect and process data, especially when it is sensitive and personal.

A pertinent example is the deployment of algorithmic decision-making. There are really two distinct breeds of system here; one that relies on lots of manual intervention and programming to develop the final algorithm and another, so-called machine learning, where the system has built up its own logic and constructed the algorithm without much (or any) human assistance. It's important to point out that 'the algorithm did it' should never be an acceptable excuse if algorithms make mistakes or create undesired, or even unexpected, outcomes. Humans, corporations, and public bodies should always be accountable for the systems they deploy. Although ensuring there is clear responsibility within an organisation deploying an algorithmic decision-making system is key to ensuring accountability, it isn't comprehensive enough. What accountability should really mean is 'an obligation to report and justify algorithmic decision-making, and to mitigate any negative social impacts or potential harms'.[27]

On the other side of the accountability equation is what the data economy should hold us accountable for. Presently, it is the digital representations of ourselves that are being held to account. If our credit profile shows that we have outstanding debt then we will be held accountable

BOX 2. FIVE ASPECTS OF ACCOUNTABILITY FOR ALGORITHMS[28]

1. **Responsibility.** It's important that those deploying these systems take responsibility for the outcomes they produce and that those affected can seek redress. For any system, there should be a named person with the authority to deal with the effects of the deployment of the algorithm.

2. **Explainability.** All decisions that an algorithmic decision system generates must be explainable to those affected

3. **Accuracy.** This principle states that no system is perfect and even the best algorithms will make mistakes. Understanding this is therefore critical and should require those deploying these systems to understand sources of potential errors and statistical uncertainty.

4. **Auditability.** Algorithms should be developed and deployed so that third parties, both private and public, can interrogate the behaviour of an algorithm.

5. **Fairness.** All algorithms decisions systems should publicly release information about any discriminatory effects.

for that, even if no debt exists in real life. For each of us, there are literally thousands of digital profiles being used to make decisions about us. Currently any business can create a digital profile on anyone, provided they can justify the data gathering under the GDPR, but they have no duty to ensure that their data is accurate. At the same time we don't have easily exercisable rights to query and correct what data is being held about us, especially since profiles are often sold multiple times to third parties. This must change if we're to ensure that we're not being held accountable for something we didn't do, or character traits that we don't exhibit.

At present, accountability is severely lacking in the data economy in two ways: how we hold systems to account and what systems hold us to account for. As the data economy grows and permeates every part of our lives, we must ensure that proper controls are put in place.

INCREASED TRANSPARENCY

The data economy is where it is in large part because the underlying architecture, the economic model, and the data collection regime are invisible to most people. It's questionable whether the digital data economy would have grown in the way that it has, had we been aware of the grand bargain in which we were exchanging our data and privacy for convenience and low-to-no-cost products and services. As US Supreme Court judge, Louis Brandeis famously quipped: 'Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.'[29] It is staggering that today 25% of us remain unaware that the core business model of digital platforms is to monetise our data, while 45% don't know that companies use that data to provide personal ads.[30] If the inner workings of the data economy were brought to the surface, it should be easier to fight for the type of economy.

We therefore need interventions that provide increased transparency in general, as well as in specific areas like data collection, data processing, the explanation of an algorithmic decision. And we need new rights, such as the right to know when we're interacting with an algorithm.

EXAMPLE 5. DECIDIM

Decidim is an open source platform that enables democratic participation and participatory budgeting in Barcelona and Helsinki. It uses the latest technology to give citizens a transparent way to engage with city administrations, while guaranteeing personal privacy and public transparency in a way private platforms don't.

Decidim taps into the potential of social networks but puts citizens in the driving seat. Citizens can choose what kind of data they want to share, with whom, and on what terms.

It is run on free software so all the code and data are accessible, reusable, and auditable with everything published and freely available in the public domain. This transparent code is in stark contrast to the dependency that comes through outsourcing tech systems to big corporate players, whose code is usually black-boxed due to commercial secrecy.

Decidim implements transparency in a number of different areas to achieve different goals. First, it creates a more transparent public administration, with a clear link between the people who voice an opinion and the responses from the city administrators. Second, the transparency of the system and how it operates ferments trust and empowers people to engage with it. Finally, the open code enables anyone with the necessary skills to independently verify that it is doing what it promises.

CONCLUSION

Following these principles when thinking about new businesses, reforming existing businesses, or considering the development and revision of policy will help ensure that the needs of people and society are placed at the centre of the data economy as it develops. These guiding principles should continue to be used, even as the technical and legal landscape shifts and develops. The structures, practices, and regulations that develop, should put the protection of people first, including their right to privacy. This should always be favoured over facilitating the needs of private companies and their constant quest for profit, or the government's desire to monitor and track elements of our digital behaviour. The stakes are just too high for us to fail.

ENDNOTES

1 The New Yorker. (2018, April 9). Briefly Noted. Retrieved from https://www.newyorker.com/magazine/2018/04/09/surveillance-valley-visionary-women-call-me-zebra-and-the-driest-season

2 Yueh, J. (2018, June 26). GDPR will make big tech even bigger. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/06/26/gdpr-will-make-big-tech-even-bigger/#528d80572592

3 Holton, K. (2018). GDPR Advertising fallout: Tech giants tighten their grip in the EU as some smaller players flee. Retrieved from https://venturebeat.com/2018/08/23/gdpr-advertising-fallout-tech-giants-tighten-their-grip-in-the-eu-as-some-smaller-players-flee/

4 Hern, A. (2018, July 5). Privacy policies of tech giants 'still not GDPR compliant'. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/jul/05/privacy-policies-facebook-amazon-google-not-gdpr-compliant

5 Hern, A. (2018, January 9). No tracking, no revenue: Apple's privacy feature cost ad companies millions. *The Guardian*, retrieved from https://www.theguardian.com/technology/2018/jan/09/apple-tracking-block-costs-advertising-companies-millions-dollars-criteo-web-browser-safari

6 Fisher, B. (2018) Ad Blocking the UK 2018. *eMarketer*. Retrieved from https://www.emarketer.com/content/ad-blocking-in-the-uk-2018

7 Tabora, V. (2018). The evolution of the internet, from decentralized to centralized. Retrieved from https://hackernoon.com/the-evolution-of-the-Internet-from-decentralized-to-centralized-3e2fa65898f5

8 Netimperative. (2018). Netflix now accounts for 15% of global internet traffic. Retrieved from http://www.netimperative.com/2018/10/netflix-now-accounts-for-15-of-global-Internet-traffic/

9 Desjardins, J. (2017). The 100 websites that rule the internet. Retrieved from http://www.visualcapitalist.com/100-websites-rule-Internet/

10 One of the most famous DDoS attacks occurred in 2010 when groups of hackers targeted Visa and Mastercard in retaliation for their decision to pull services from Wikileaks. The action led to Visa and Mastercard being unable to process some interactions.

11 An example could be running your own server on Mastodon, the decentralised Twitter, or running your own node on the Bitcoin network.

12 Barabas, C., Narula, N., & Zuckerman, E. (2017). Defending Internet Freedom through Decentralisation: Back to the future? *MIT Media Lab*. Retrieved from https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/59ae908a46c3c480db42326f/1504612494894/decentralized_web.pdf

13 Zuckerman E (2017) Mastodon is big in Japan. The reason why is … uncomfortable, retrieved from http://www.ethanzuckerman.com/blog/2017/08/18/mastodon-is-big-in-japan-the-reason-why-is-uncomfortable/

14 Privacy Law and Business. (2018). First UK collective action cases in the pipeline. Retrieved from https://www.privacylaws.com/Publications/enews/UK-E-news/Dates/2018/8/First-UK-collective-action-cases-in-the-pipeline/

15 Eight million downloads per day x 10 minutes to read the terms = 152.2 years.

16 Dormon, B. (2012, April 12). Adobe demands 7,000 years a day from humankind. *The Register*. Retrieved from https://www.theregister.co.uk/2012/12/04/feature_tech_licences_are_daft?page=1

17 WolfieChristl. (2018, December 6). Internal FB docs, does anyone know: - What are FB apps 'generating TPV'? - What are 'noisy' apps? - Do we have any idea which apps are T0/T1? Device integrations+? - Is it possible that 'Salesforce' isn't just internal wording but refers to the company?" [Twitter Post]. Retrieved from https://twitter.com/WolfieChristl/status/1070695293967130632?s=03

18 McCann, D. & Hall, M. (2018). Blocking the Data Stalkers. London: NEF. Retrieved from https://neweconomics.org/2018/12/blocking-the-data-stalkers

19 The Economist. (2018, January 11). Should Internet firms pay for the data users currently give away? Retrieved from https://www.economist.com/news/finance-and-economics/21734390-and-new-paper-proposes-should-data-providers-unionise-should-internet

20 Posner, E. & Weyl, E. (2018). Radical Markets: *Uprooting Capitalism and Democracy for a Just Society*. Princeton, Princeton University Press

21 Lanier, J. (2014). *Who Owns The Future?* London: Penguin.

22 McCann, D. & Hall, H. (2018). Blocking the Data Stalkers. London: NEF. Retrieved from https://neweconomics.org/2018/12/blocking-the-data-stalkers

23 Schiller, B. (2018). Can this app that lets you sell your health data cut your health costs? Retrieved from https://www.fastcompany.com/40512559/can-this-app-that-lets-you-sell-your-health-data-cut-your-health-costs

24 Medical Research Council. (n.d.). Value of using data. Retrieved from https://mrc.ukri.org/research/initiatives/health-and-biomedical-informatics/value-of-using-data/

25 NESTA (2018) MIDATA.coop. Retrieved from https://www.nesta.org.uk/feature/me-my-data-and-i/midatacoop/

26 Nesta. (2018). MIDATA.coop. Retrieved from https://www.nesta.org.uk/feature/me-my-data-and-i/midatacoop/

27 Diakopoulos, N. & Friedler, S. (2016). How to hold algorithms to account. Retrieved from https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/

28 Inspired directly from: Diakopoulos, N. & Friedler, S. (2016). How to hold algorithms to account. Retrieved from https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/

29 Braneis, L. (1914). *Other People's Money and How the Bankers Use it*. New York: Frederick A Stokers.

30 Doteveryone. (2018). People, Power and Technology: The 2018 Digital Attitudes Report. Retrieved from http://attitudes.doteveryone.org.uk/files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf

NEW ECONOMICS FOUNDATION

WWW.NEWECONOMICS.ORG
info@neweconomics.org
+44 (0)20 7820 6300 @NEF
Registered charity number 1055254

WRITTEN BY:
Duncan McCann

COVER IMAGE:
www.istockphoto.com/monsitj

PUBLISHED:
April 2019

ACKNOWLEDGEMENTS:
Thanks to the Joseph Rowntree Charitable Trust for funding NEF's work on the digital economy.