DATA-POP ALLIANCE

Vodafone Institute for Society and Communications

digitising europe

Emmanuel Letouzé and Nuria Oliver

Sharing is Caring

Four Key Requirements for Sustainable Private Data Sharing and Use for Public Good

November 2019

Content

1. Context and questions

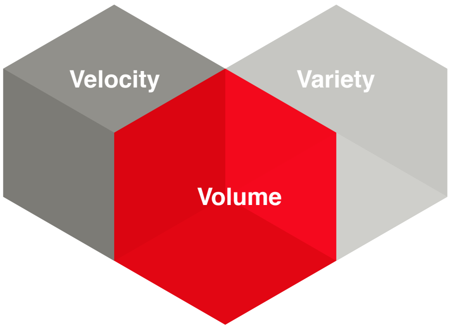
How data are shared and used will determine to a large extent the future of democracy and human progress. A first imperative is to understand the key features of the ongoing "Data Revolution", which is not just about data.[1] The Data Revolution is fuelled by three main factors. The first is the exponential growth in the generation of digital human behavioural data, or "digital crumbs",[2] resulting from our interactions with digital devices and services, the digitisation of the physical world by means of sensors, and the development of the Internet of Things (IoT).[3] The second is the development of sophisticated technological and human capacities to store, structure and make sense of these data, including cloud computing, high-performance and large-scale computing at an affordable cost, and new data-driven machine-learning approaches, such as deep-learning. The third factor is the growing role and interactions of communities of providers, analysts, users and regulators with these new crumbs and capacities, all of whom collectively shape what is known as the data econo-

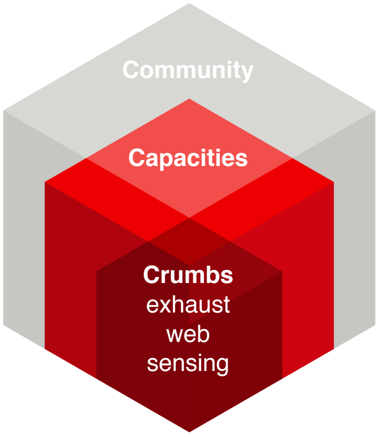
1 https://www.washingtonpost.com/blogs/post-live/wp/2016/05/05/meet-professor-gary-king/

2 Brockman, John, 2012. Reinventing Society in the Wake of Big Data. A conversation with Alex "Sandy" Pentland. United States: The Edge.

3 Including Internet of Things devices. In 2020, according to a recent DOMO report, 1.7MB of data will be created every second for every person on earth, contributing to a total of 40 zettabytes of data, according to IDC. DOMO INC. 2018. Data Never Sleeps 6.0. American Fork, UT: DOMO.

Figure 1: Evolution of the definition of Big Data





circa 2010: the V's of Big Data

now: the C's of Big Data

Source: Emmanuel Letouzé

my.[4] These „three Cs" – standing for Crumbs, Capacities and Community — are the constitutive elements of a revolution that is already changing our daily lives, businesses, government operations and societies at large.[5] While the economic impact of such a revolution has been estimated to be in the hundreds of millions of euros in Europe, most of this impact has been quantified from a business perspective, given that a large percentage of these massive amounts of data is collected and controlled by private companies.

Looking ahead, it is clear that one of the biggest questions posed to all stakeholders, policymakers in particular, is whether and how these sensitive data – and/or the insights they contain – should be shared to maximise their potential for public good. In more specific terms, what are the technological systems, governance standards, economic models and ethical frameworks that ought to be considered in order to foster technological, economic and social innovation from these data? Shaping a market for data – understood broadly as the mechanism for matching supply and demand – while ensuring that the Data Revolution benefits societies and citizens broadly, and not just large companies, small fractions of society and surveillance actors, is of the utmost necessity.

The term "Data Revolution" became a common phrase in international development circles almost a decade ago. In 2012, the UN published its first report on "Big Data for Development",[6] followed in 2013 by another UN report called "Data Revolution for Sustainable Development"[7]. That, in turn, was followed by another report in 2015 from a group with links to the UN, which argued that data should be at the heart of public policies and programs in support of the 2030 Sustainable Development Agenda and its 17 Sustainable Development Goals (SDGs). The UN subsequently organized two editions of the "World Data Forum" in 2017 and in 2018 in South Africa and Dubai, while the third edition is scheduled to take place in Switzerland in October 2020.[8] The 2018 Forum wrapped up with the launch of the Dubai Declaration, which aims to increase financing for better data and statistics for sustainable development.[9]

4 According to the European Commission, the data economy will surpass 700 billion euros by 2020 and the World Economic Forum predicts that 60-70% of growth in global GDP will be due to "data-driven, digitally enabled networks and platforms". World Economic Forum. 2018. Our Shared Digital Future: Building an Inclusive, Trustworthy and Sustainable Digital Society. Cologny/Geneva, Switzerland: World Economic Forum.

5 White Paper DPA 2015; Viktor Mayer-Schönberger and Kenneth Cukier (2013) Big Data: A Revolution That Will Transform How We Live, Work and Think. John Murray. ISBN 9781848547926.

6 Letouzé, Emmanuel. 2012. Big Data for Development: Challenges & Opportunities. New York, NY: United Nations Publications.

7 Panel Secretariat led by Dr. Homi Kharas. 2013. A New Global Partnership: Eradicate poverty and transform economies through sustainable development. The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda. New York, NY: United Nations Publications.

8 The third UN World Data Forum will be hosted by the Federal Statistical Office of Switzerland from Oct. 18-21, 2020, with support from the Statistics Division of the UN Department of Economic and Social Affairs, under the guidance of the United Nations Statistical Commission and the High-level Group for Partnership, Coordination and Capacity-Building for statistics for the 2030 Agenda for Sustainable Development. For more information, please visit https://unstats.un.org/unsd/undatafo-rum/index.html.

9 UN Editor. 2018. World Data Forum wraps up with a declaration to boost financing for data and statistics. New York, NY: United Nations Department of Economic and Social Affairs.

This interest has largely stemmed from early evidence of the value of insights gleaned from the computational analysis of our digital crumbs. Because of the penetration of mobile phones in both developed and developing countries,[10] the majority of early publications, pilots and initiatives on this topic have relied on data passively collected by the mobile network infrastructure for billing and other internal purposes (Call Detail Records (CDRs) or network probes). These studies have showed how analysing human behaviours captured by these datasets could inform natural disaster and emergency response, improve transportation, complement official statistics, help fight epidemics, understand crime, estimate socio-economic development, foster financial inclusion, and so forth[11]. Dozens of scientific publications have stemmed from “Data Challenges”, such as those organized by Orange, Telefonica and Turkcell, but also by banks such as BBVA. Others have resulted from bilateral agreements or internal projects. (see Box 1).

These initiatives have reflected and stirred a growing desire for accessing and analysing those new kinds of data – sometimes compared to a “new oil”[12] that can be extracted and refined to fuel more efficient, data-driven, evidence-informed decision-making systems. The oil analogy may seem tired or misguided[13] (also because data are non-rivalrous and non-finite). However, it does serve to highlight some of the risks inherent in data, including the fact that once data are leaked, they are very difficult to reclaim. Will our datafied world be as extractive as the oil industry? Will data increase power imbalances and further consolidate monopolies? Will it fuel corruption, benefit autocrats and undermine democratic principles?[14] Will it kill privacy? Will automated decision-making and so-called „black box algorithms“ lead to the demise of democracy as government by discussion? These fears and criticisms, many legitimate, have started giving data and data-driven algorithms a bad name. They have even led many people to push back on attempts to foster more data-driven or data-informed decisions, especially in contexts where data literacy and culture are often weak.

Cautious optimists, such as ourselves, argue that these legitimate concerns must inform, rather than impede, attempts at making data a key force for human progress. We believe that these new kinds of crumbs and capacities have the potential to help reduce pervasive limitations in human decision-making and governance – including corruption, cognitive biases, misinformation, greediness and conflict of interests – to build healthier communities. We furthermore believe that Europe is well situated to lead the way in that domain, including by building on and promoting the vision behind the GDPR, a vision according to which data subjects and data generators have more control over how data pertaining to themselves are collected, shared and used.

Data- or evidence-informed decision-support systems, where machine-learning algorithms might play a central role,

10 World Bank Team led by Mishra, Deepak & Deichmann, Uwe. 2016. World Development Report 2016. Digital Dividends Overview. Washington, DC: International Bank for Reconstruction and Development / The World Bank.

11 Blondel, Vincent D., Decuyper, Adeline & Krings Gautier. 2015. A survey of results on mobile phone datasets analysis. Belgium: EPJ Data Sci.

12 The Economist. 2017. The world’s most valuable resource is no longer oil, but data. United States: The Economist.

13 García Martínez, Antonio. 2019. No, Data Is Not the New Oil. San Francisco, CA: Wired

14 O’Neil, C. 2016. Weapons of math destruction: how big data increases inequality and threatens democracy, New York, NY: Crown, and Y. N. Harari. 2018. Why Technology Favors Tyranny. Washington, DC: The Atlantic.

Box 1: Defining private data sharing for public good

1 Insights or knowledge derived from data: new knowedge or understanding derived from the analysis of the data

2 Processed or analyzed data; data that has been analyzed and visualized

3 Preprocessed data: raw data that has been prepared for analysis

4 Raw data: data directly captured by a sensor or service and that has not been processed

In this paper, “private data” is understood as data collected and controlled by private organisations, in most cases private commercial / for profit companies, about the activities of their customers. Examples include cell phone metadata, credit and other financial transactions, social media data, search engine data, mobile apps data, data captured by mobile operating systems and wearable or IoT devices, among others. These can be processed and shared according to different levels of abstraction.

However, sensitive data about beneficiaries collected by not-for-profit organizations, such as UN humanitarian agencies, may also be considered private data, with different political and economic sensitivities. Private data and personal data are not synonymous since pseudonymised aggregated data may cease to be personal data but remain referred to as private data to characterise their origin. “For public good” refers to the objective of using insights resulting from analyses of these data to advance societal welfare, including but not limited to the achievement of the 17 Sustainable Development Goals (SDGs).

have been referred to by some authors as "Human AI" systems.[15] Human AI systems refer to groups or societies where collective decisions are taken and evaluated based on data that is analysed by humans and/or AI algorithms. They seek to learn from their performance (often with input from humans in the form of penalties and rewards) what seems to produce good outcomes versus what does not. To function, these systems need to be able to access and analyse a wide variety of available digital crumbs using state-of-the-art capacities, allowing communities to make better decisions for themselves. Human AI is consistent with, but broader than, the „human-centric AI" approach promoted by the European Commission. The term „human-centric AI" refers to using AI in ways that reflect core human values. Human AI adds to this concept a vision whereby humans alone, or with the help of AI systems, make decisions based on evidence, encouraging what seems to yield good outcomes while seeking to discourage what doesn't—which in some cases could include the use of AI systems altogether.

Today's world is quite far from this vision. To date, there have been very few examples of real-world systems which systematically leverage large-scale human behavioural data to make better decisions for the public good. Indeed, many public policies run counter to what basic facts would suggest.

Major hurdles to data-driven public decision making have included the difficulties associated with giving third parties access to these data without creating risks to individual or group privacy, the lack of well-defined ethical principles, potential legal and regulatory barriers and the existence of competing commercial interests. The bulk of these data are sensitive, valuable personal data collected and controlled by private companies. What frameworks and standards may allow sharing these data at scale in an ethical and privacy-preserving manner? What kinds of financial models, incentives and regulations may make data sharing for public good sustainable? And even if those data (or statistics and insights derived from it) become available, how can we ensure that public administrations have the appropriate capacities and culture to adopt this new method of making decisions? After all, the public sector already has access to large amounts of data that are not touched or acted upon.

These questions and observations suggest that there are still significant obstacles on the path from data to evidence-informed decisions and outcomes. Simply assuming that more and better data would easily and immediately lead to both better decisions (including from governments) and better outcomes overlooks important lessons from human history, psychology and political economy. Over at least the past three centuries, it is difficult to argue that the greater availability of data and information to larger numbers of people has helped better distribute human knowledge and wealth. But we also know that it usually takes more than facts to change people's minds,[16] and that yesterday, today and, most likely, tomorrow, most individuals and institutions in positions of power will try to preserve that power. This often means disregarding or tweaking data, facts and statistics to that end. Consequently, if we are interested in the end goal — that of improving the world through data and not simply cracking the major first-mile problem of data access – we must consider the entire spectrum of hurdles and pathways that would allow our data crumbs to improve our communities. We argue that this requires supporting the deployment of sustainable systems and standards, but also the development of capacities and incentives to access, analyse and put data to use.

Thus, while this paper focuses on data access and sharing— the beginning of the causal chain — it does so with an eye on data usage and impacts — the end of the chain — and how considerations for the latter impact reflections and decisions on the former. Likewise, while it discusses data sharing "for the public good",[17] it cannot do so in a vacuum. It must also take into account data for profit activities that are part of companies' efforts at monetising data they collect and control (also called „valorising"—i.e. turning these data into economic value). It quickly becomes clear that the question as to whether and how privately collected and controlled data could or should be shared for the public good is not merely a technical or even legal one. Rather, it is a complex, multi-faceted issue that also gets deep into political, social, ethical and business matters.

In this paper, we provide an overview of the current state of play in private data sharing for the public good. We highlight gaps and needs in addition to describing four main requirements and one specific example that may help current and future digital, datafied societies fully benefit from the immense potential that large-scale personal data hold. We conclude with seven recommendations for actions that we believe would help realise the immense potential of using privately held data for public good.

15 Letouzé, Emmanuel & Pentland, Alex. 2018. Towards a Human Artificial Intelligence for Human Development. ITU Journal: ICT Discoveries.

16 Kolbert, Elizabeth. 2017. Why Facts Don't Change Our Minds. New discoveries about the human mind show the limitations of reason. New York, NY: The New Yorker.

17 We consider "data sharing for public good" to be effort to use data for a positive impact on society. Note that also we refer to these efforts as "social good" and "public interest" interchangeably.

2. Characteristics, benefits and limits of current private data sharing models and efforts for public good

To date, five major private data-sharing models have been used, each with specific characteristics, benefits and limitations:

1. **Limited data release**
2. **Remote access**
3. **Application Programming Interfaces (APIs) and Open Algorithms**
4. **Pre-computed indicators and synthetic data**
5. **Data collaboratives or cooperatives**

These five data-sharing models can be organised and visualised in a graph, with levels of security and scalability on both axes (see Figure 2).

1 The first model is the **limited data release** model, a "one-to-many" modality where private companies prepare or "package" data and then provide one or more proprietary datasets to selected groups — typically following some screening and after a contract or NDA (non-disclosure agreement) is signed. Examples of this are the aforementioned "Data Challenges". These arrangements have been – and, in some cases, remain – key to creating awareness, but they are costly and time-consuming to organise. They also imply that datasets, which are, of course, pseudonymised and aggregated to levels considered safe from a privacy standpoint, will be „in the wild" for unknown periods of time, with little to no possibility of tracking their whereabouts. Another limitation is the fact that in most cases, local communities are not involved in the projects and their long-term impacts seem limited. Finally, while this access model has helped with understanding the value of data for public good, it does not allow for an ongoing analysis of the data over time.

2 The second model is through one-to-**one or one-to-few contractual agreements with specific individuals or institutions** (governments or NGOs), who are then allowed to analyse proprietary data, after having signed an NDA, for a particular purpose related to the social good and possibly for a limited period. A common approach involves granting **remote access** to (typically) pseudonymised data to these authorised parties. In some cases, however, access to pre-packaged datasets with specific features is granted. Organisations like United Nations Global Pulse, Flowminder and Data-Pop Alliance (DPA) have carried out many projects and pilots using this model. DPA, for example, is running pilots with the United Nations Economic and Social Commission for Western Asia (UNESCWA) in Lebanon to understand the living conditions of Syrian refugees and with the United Nations Development Programme (UNDP) in Moldova to study urban mobility in the country's capital. This form of data sharing can yield impressive results and build trust, and it is relatively safe. But it is not built for scaling and tends not to be very participatory.

3 A third model is **few-to-many access through Application Programming Interfaces (APIs) and Open Algorithms.** This approach enables the use of privately held data without the data ever leaving the premises of its owners/custodians. This is advantageous given the high volume and dynamic nature of the data. Both pre-computed indicators or richer question-and-answer access models can be implemented by means of an API. This means that users can either send code and/or algorithms to a server via an API in order to get an answer to a query, or they can simply pose a question which the server is prepared to answer. This modality allows for sharing data-based insights rather than unprocessed or raw data and is a type of access enabling a few-to-many data sharing model. Examples of the use of APIs for data access include the GSMA Big Data for Social Good Initiative and the OPAL project, which we describe in detail below. APIs enable queries of pre-computed indicators or a more interactive, granular and dynamic question-and-answer model, for which OPAL is a good example, as discussed in Section 4.

4 In some cases, **pre-computed indicators** are shared with interested parties in a one-to-one or one-to-few sharing model. Alternatively, **synthetic data** with similar statistical properties as the original data might also be shared. In this case, a one-to-many sharing model could be adopted.

5 Yet another model involves **data cooperatives and data collaboratives**, (or „spaces") which are collaborations between participants willing to exchange data to create public value. This model is typically a few-to-few / many-to-many model, given that any contributing member is able to access the data shared by others. It must be noted that these approaches must rely on one of the other data sharing modalities for data to actually be shared. As such, they are less of a model to facilitate data sharing and more of an institutional arrangement to incentivise data sharing. Data cooperatives are especially interesting due to the vision offered by their proponents of existing institutions, such as credit unions, playing a similar societal role as that of banks, but instead of handling money, they are handling data.[18] This model entails consensual data pooling enabled by privacy-preserving technologies, such

Box 2: Telco Data Challenges and initiatives

Mobile network operators have been among the most active private stakeholders in this modality of data sharing. Orange's Data for Development (D4D) Challenges in Ivory Coast (2013) [cite] and Senegal (2015) [cite] were among the first and most important data sharing challenges. They enabled hundreds of researchers to analyse aggregated and anonymised mobile data for a variety of public good purposes, including financial inclusion, socio-economic development, climate change, natural disasters, transportation, national statistics and public health. Telefonica, Telecom Italia and Turkcell also organized their own Data for Social Good challenges in London, Trentino and Turkey. Vodafone has also collaborated with relevant NGOs globally, such as Flowminder in Ghana, while the Vodafone Institute has led the Digitising Europe initiatives for several years, which have included contributions from the Data-Pop Alliance.

18 Walsh, Dylan. 2019. How credit unions could help people make the most of personal data. Boston, MA: MIT Management Sloan School.

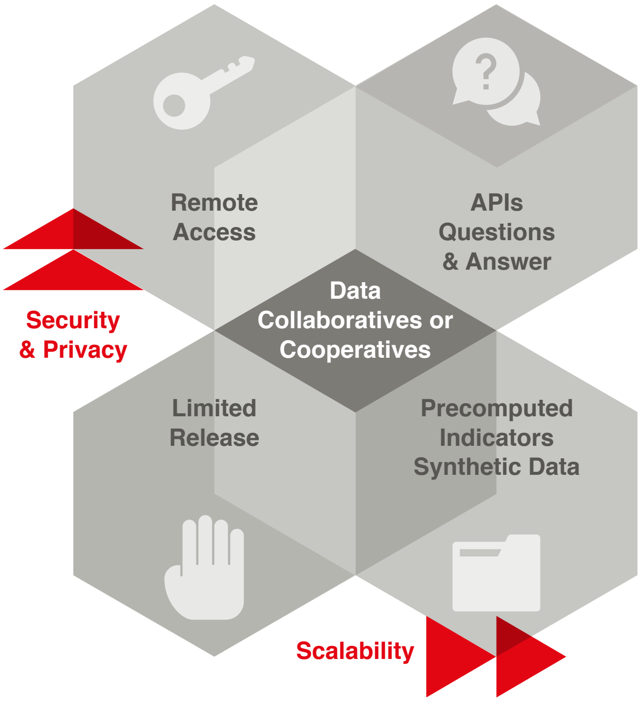
as differential privacy.[19] In data cooperatives, "individuals would pool their personal data in a single institution — just as they pool money in banks — and that institution would both protect the data and put it to use". In such a data cooperative, "while companies would need to request permission to use consumer data, consumers themselves could request analytic insights from the cooperative". Furthermore, what is shared in the data cooperative model are typically aggregated insights and not the raw or even pseudonymised data.

Defining which modality to use depends on a range of factors, including the technical capacities of both the user and the data owners/custodians, the level of granularity needed, the type of data being shared and the expected use for the data, among many other considerations. While the modalities mentioned above provide a broad picture of data-sharing models, new models will emerge to make data sharing more accessible – in terms of frequency and ease of sharing small and large volumes of data – as stakeholders increasingly recognise the potential that bridging institutional data-silos may hold for the public good. A recent and potentially emerging sharing modality, proposed by the Open Data Institute (ODI) in the UK, is the concept of data trusts.[20]

According to the ODI, a data trust is "a legal structure that provides independent stewardship of data". Data trusts allow people or organisations that generate data to give some control over their data to a new entity (the trust) so it can be used to provide services or yield benefits to themselves or to others. Precisely how the data trusts will access and transfer the data from where it is being generated has yet to be defined. Data trusts can be used for data governance, since they can be responsible for stewarding, maintaining and managing how data is used and shared (who has access to it and for which purposes). As part of a UK government-funded research program, the ODI recently carried out three data-trust pilots, which ran from December 2018 to March 2019 and focused on three use cases of public good: improving public services in Greenwich, tackling the illegal wildlife trade and reducing food waste. The results of these pilots have helped the ODI define their recommendations for the design and development of a data trust in the city of London.

This and many more pilots exploring modalities for data-sharing are taking place in Europe, where interest in sharing data across stakeholders is especially high. In fall 2018, for example, the European Commission created a High-Level Expert Group (HLEG) on Business-to-Government Data Sharing, with representatives from academia, NGOs and industry.[21] The HLEG is expected to produce a report with key recommendations regarding data sharing from private companies to public stakeholders by early 2020.[22] Additionally, an international workshop exploring private data sharing also took place in September 2019 at Eurostat, whose teams are developing a methodological and technical framework to derive statistics from data generated by mobile operators.[23]

Figure 2: Five models for the privacy-conscientious use of mobile phone data



Adapted from https://www.nature.com/articles/sdata2018286/figures/1

Yet, while there is significantly higher public awareness of the opportunities that private-to-public data-sharing frameworks could unlock, to date there are no common standards, viable financial models, consistent regulations, multi-stakeholder coordination or ambitious multi-year projects to fully realise such opportunities. Solutions seem to be in sight, but significant work is required to assemble all the pieces of the puzzle.

In this context, we describe four key requirements that we believe must inform European efforts to ensure that private data are shared and used for the public good in a safe, ethical and sustainable manner.

19 Dwork, Cynthia and Roth, Aaron. 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. Philadelphia, PA: University of Pennsylvania.

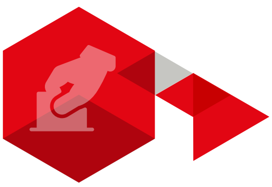
20 Hardinges, Jack & Wells Peter. 2018. Defining a 'data trust'. London, UK: Open Data Institute.

21 European Commission. 2018. Commission appoints Expert Group on Business-to-Government Data Sharing. European Union.

22 One of the authors of this paper, Dr. Nuria Oliver, is a member of the High-Level Expert Group on Business to Government Data Sharing at the European Commission.

23 Ricciato, Fabio, Lanzieri, Giampaolo & Wirthmann, Albrecht. 2019. Towards a methodological framework for estimating present population density from mobile network operator data. Luxembourg, LU: European Commission – EUROSTAT.

3. Four key requirements for sharing and using private data for public good



3.1. Get the politics right

Sharing private data for public good involves three groups of actors: private organisations holding the data; institutions expressing data demands on behalf of societies; and individuals whose data is the element of interest. These parties have potentially conflicting interests, constraints and priorities, some of which might be more negotiable than others. This observation suggests that there is a political dimension to the challenge of data sharing. Getting the politics right requires striking a balance between the private, the public (e.g. governments) and the individuals' interests, which implies understanding their underlying dynamics.[24]

The first group of stakeholders is private organisations, which in most legal frameworks are the legal owners or custodians of the data of interest. Even though corporations increasingly monetise consumer data via their own operations and services, or even by selling them, they typically worry about sharing data externally for a variety of reasons. These include perceived reputational and legal risks (if something goes wrong or if the project gets bad press), financial costs (including costs associated with setting up sharing infrastructures), and fears that sharing data may negatively influence the business prospects of selling them in the short, medium and long term.[25] Some companies feel they are sitting on gold mines –or oil fields– and they want to keep their data inside their vaults (servers) until they figure out a business model.

The second group of stakeholders encompasses the institutions that demand access to private data and/or insights these data contain for public good. Such institutions could be governmental — such as ministries, local governments and National Statistical Offices (NSOs) — or they could come from academia or civil society (including private universities). NSOs are a good example to illustrate the main considerations and constraints of this group.

24 Letouzé, Emmanuel, Kammourieh, Lanah & Vinck, Patrick. 2015. The Law, Politics, and Ethics of Cell Phone Data Analytics. Boston, MA: Data-Pop Alliance.

25 https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf

Most NSOs around the world would want to access these data for statistical purposes — to calculate population density or poverty estimates between censuses, for example. Very few, though, have been successful in doing so. Thus, some NSOs have proposed the use of regulations as a tool to incentivise or compel private companies to share their data with them. The case for NSOs being able to rely on these data to provide a better picture of reality to decision-makers and citizens is strong. Nonetheless, if this is done without appropriate consultation and in the absence of appropriate technological and governance safeguards, there are risks in potentially alienating private companies, breaching consumer privacy and breaking citizens' trust. NSOs also have concerns about reputational risks if it turns out that using these data leads to unintended consequences. One example is the recent negative press received by a project undertaken by the Spanish Institute of National Statistics due to their having leveraged aggregate insights derived from mobile data without the knowledge or explicit consent of mobile users.[26] Another fear is that of developing partnerships and investing in the use of private data absent guarantees that the flow of data will stop at some point in the future. Hence, the focus on regulations and partnerships to address this fear.

Last, but not least, are the individuals whose data are already being analysed for many purposes, presumably with their consent (we click "accept" or sign contracts that give companies rights over our data) but possibly, or typically, not with their understanding of what data is being captured and how it is being used. Key principles and rights, such as transparency, fairness, autonomy and privacy, would need to be demonstrably preserved, as discussed in Section 3.3. Given the value of the data, several projects have proposed the creation of personal data markets [27] where individuals have control over their own data and decide whom to share it with and at what cost.

The GDPR and the ePrivacy Directive place a welcome premium on obtaining consent from users and requiring data controllers to put measures in place to keep track of the whereabouts of consumer data. However, the GDPR also allows for the lawful processing and sharing of private data for some uses, including the computation of statistics that are no longer considered personal data, leaving open many avenues for research and policymaking purposes without requiring consent. We believe that in the future, however, all data-sharing initiatives should make it possible to opt out, regardless of the usage, with adequate communication. This creates the risk of attrition, which has been demonstrably significant in situations when active consent has been sought.

A key challenge will be to convince data subjects that it is not only safe, but also in their interests to agree to make their data available for the purposes of public good – either by opting in or not opting out — as we do in insurance schemes. The aforementioned example of data cooperatives presents a model where individuals and institutions would agree to share their data for common objectives with the associated rights. However, given concerns expressed in many countries, it seems that significant efforts still need to be undertaken to show evidence of returns and ensure that the technology and science are both sound and safe to generate public trust. Thus, the next requirement concerns the necessary technology and science to enable turning data into reliable and actionable knowledge.

3.2. Get the technology and science right

Getting the technology and science for private data sharing right means first and foremost that decisions about whether and how to share data necessarily be informed by state-of-the art scientific knowledge – knowledge regarding not only what methods work best on which data and for which purposes, but also regarding the limitations and risks associated with the use of such methods. Like all technologies, Big Data analysis can and will have both great positive and potentially negative consequences. Maximising the former while minimising the latter requires having a solid understanding of the technology behind the technology – the technological and scientific underpinnings and inner workings of data science.

A particularly important set of risks concerns computational violations of individual privacy stemming from possible re-identification. A few years ago, "anonymising" data — meaning replacing information that identified a specific individual such as their name, date of birth, phone number, etc., with a unique identifier (hash) — was considered to be safe, as long as the key or anonymisation procedure could not be found. It was also believed that coarsening the data would make it even more difficult to re-identify people

26 https://www.elconfidencial.com/tecnologia/2019-10-29/ine-operadoras-recopilacion-datos-moviles-proteccion-ley-es_2304120/

27 Caraviello, Michele; Lepri, Bruno; de Oliveira, Rodrigo; Oliver, Nuria; Sebe, Nicu & Staiano, Jacopo. 2014. Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data. Seattle, WA: UbiComp 2014 - Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing.

in an anonymised dataset. Research has since shown that individual behaviours are so unique that it is often theoretically possible to single out an individual, even with coarsened data.[28] This is because there can only be one individual displaying the specific features observed in the dataset. If that individual is also present in another dataset containing personal information, and the two datasets can be matched, the individual would be fully re-identified.[29] Research is currently ongoing to understand the limits of human privacy and how it can be protected.[30] But the current state of knowledge is clear: Anonymising personal data is not necessarily enough to protect individual privacy.[31]

One promising technical approach to preserving privacy is called „differential privacy".[32] Differential privacy is a mathematical definition of privacy that enables the statistical analysis of datasets that may contain personal data in such a way that when looking at the output of such an analysis, it is impossible to determine whether any specific individual's data was included in the original dataset or not. The guarantee of an algorithm applied to a dataset that is differentially private is that its behaviour does not change when an individual is included in or excluded from the dataset. This guarantee holds for any individual and any dataset. Hence, regardless of the specific details of an individual's data (even if such an individual is an outlier), the guarantee of differential privacy should still hold.

One application of differential privacy is in the context of data sharing. The most studied use case is a statistical query release, where external parties can perform specific counting queries (e.g: How many people in the dataset live in Madrid?) and receive answers that have a small amount of random noise. Differentially private algorithms can tackle many of these queries such that any researcher who might receive the approximate answers would reach the same conclusions as if (s)he had access to the data. Beyond these simple statistical queries, there are now examples of differentially private algorithms in game theory, machine learning and statistical estimation, all of which are of relevance to the data-sharing use cases for public interest.

Obviously, the larger the dataset, the higher the guarantees of differential privacy, because as the number of individuals in a dataset increases, the impact of any single individual on the aggregate statistical results diminishes. There are examples of interfaces that would enable access to private data while providing strong privacy protections using differential privacy, such as the Private data Sharing Interface (PSI) project at Harvard.[33]

Like all technologies, Big Data analysis can and will have both great positive and potentially negative consequences. Maximising the former while minimising the latter requires having a solid understanding of the technology behind the technology

Another technical way to mitigate privacy risks is to share only aggregated results and insights derived from analysing the data, such as statistical indicators. Doing so is no panacea, but it greatly reduces the risk of re-identification. Ongoing research is being conducted to both understand future weaknesses and possible technical remedies.[34]

Beyond privacy, the use of large-scale human behavioural data for the public good is still a nascent field. While there are promising results in the research literature, it is still an active research area. There are several technical and scientific challenges we would like to highlight: a lack of ground truth,[35] that would enable the proper validation of supervised, data-driven models; difficulties with real-time access to and analysis of data, despite the fact that in some impactful use cases, such as in the case of natural disasters, real-time access would be imperative; the impossibility of inferring causality, instead merely highlighting correlations, with the implications that this may have for policy- and decision-making; the potential lack of representativeness of the available data, its generalisation capabilities and inherent biases; the nonexistence of certification

28 Blondel, Vicent D., De Montjoye Yves-Alexandre, Hidalgo, Cesar A. & Verleysen Michel. 2013. Unique in the Crowd: The privacy bounds of human mobility. Belgium: "Communauté française de Belgique" on Information Retrieval in Time Evolving Networks.

29 Sloane, Tim. 2019. Another Great Argument for Synthetic Data and Self-Sovereign Identity. United States: Payments Journal; Kolata, Gina. 2019. Your Data Were 'Anonymized'? These Scientists Can Still Identify You. New York, NY: The New York Times.

30 Hendrickx, Julien M., de Montjoye Yves-Alexandre & Rocher, Luc. 2019. Estimating the success of re-identifications in incomplete datasets using generative models. Berlin, Germany: Nature. || Sloane, Tim. 2019. Another Great Argument for Synthetic Data and Self-Sovereign Identity. United States: Payments Journal || Kolata, Gina. 2019. Your Data Were 'Anonymized'? These Scientists Can Still Identify You. New York, NY: The New York Times.

31 Brogan, Caroline. 2019. Anonymising personal data ,not enough to protect privacy,' shows new study. London, UK: Imperial College London.

32 Dwork, Cynthia & Roth, Aaron. 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. Philadelphia, PA: University of Pennsylvania.

33 Gaboardi, Marco, Honaker, James, King, Gary, Nissim, Kobbi, Ullman, Jonathan, Vadhan, Salil, and Murtagh, Jack. 2016. PSI (Ψ): A Private data Sharing Interface. New York, NY: Harvard.

34 Kolata, Gina. 2019. You Got a Brain Scan at the Hospital. Someday a Computer May Use It to Identify You. New York, NY: The New York Times.

35 Ground truth is a term used in various fields to refer to information provided by direct observation (i.e. empirical evidence) as opposed to information provided by inference (e.g. by a machine learning algorithm). In machine learning, ground truth is used to train and validate supervised models.

mechanisms to guarantee the quality of the algorithms applied to the data; and the lack of transparency and interpretability of complex machine-learning algorithms, such as deep neural networks.

Moreover, using private data for public good typically entails combining datasets from different sources, which might have been captured at different moments in time with different temporal and spatial granularities and varying levels of noise. Combining such datasets in a scientifically sound way is an active study focus in the area of multi-modal or multi-source data analysis.

If we return to our example of National Statistical Offices, they also face technical challenges. Some official statisticians remain sceptical that the data would be useful due to limitations in data quality, including potential biases. Many NSOs are subject to human and technological capacity constraints along with, more broadly, imbalances of power vis-à-vis large private companies, which limits their ability to easily access private-sector data. Additional technical challenges stem from the lack of the necessary technology infrastructure and human capacity to be able to systematically store, process and use the insights derived from the data. Appropriate investments in human resources and infrastructure would be necessary to successfully carry out projects in this space, and they would need to be allocated prior to the inception of any project. Data, software and hardware are dynamic. Therefore, all projects need teams of experts dedicated to them on a continuous basis.

When dealing with data about humans which are then used to make decisions that impact the lives of potentially millions of people, numerous governance challenges and ethical dilemmas emerge.

The choice of data-sharing model – of the five models described in Section 2 – will determine what technical solution might be the most appropriate. Based on our experience, we believe that the fourth model (using APIs and Open Algorithms) has many of the features required to tackle these daunting technical challenges. This belief stems primarily from the fact that data does not need to leave the owner's servers, with the user instead being provided with aggregates or indicators. Additionally, this model's reliance on APIs and Open Algorithms to receive data means that queries can be made in a variety of systems, regardless of internal architectures.

Recommendations regarding the technology and the science of data sharing include: (1) creating and using the best knowledge and state-of-the-art technology, carefully curated based on expert knowledge of data science; (2) opting for open source as much as possible to enable information and knowledge sharing, transparency, adaptation, and the facilitation of redress when needed; (3) heavily investing in fundamental and applied research on this area so that Europe closes its current investment gap relative to the US and China; (4) and developing appropriate technological and governance systems and standards that will allow adaptation and auditing but will not impede data sharing and use, nor will it kill innovation and progress. As such, the next requirement is getting the governance and the ethics right.

3.3. Get the governance and the ethics right

When dealing with data about humans which are then used to make decisions that impact the lives of potentially millions of people, numerous governance challenges and ethical dilemmas emerge.

In this context, a simple guiding principle could be to follow what humanitarians call the "first, do no harm" principle. Today, we have a good sense of the risks that Big Data and Artificial Intelligence pose to privacy, equity, fairness and transparency to name a few areas—even when a project starts with the best of intentions. How can we be sure that sharing and using private data will do no harm? Will automated, data-driven decisions be outside of our control? Who is accountable for such decisions in cases where they may be the result of analysing several datasets by complex software and social systems developed by different parties? Will these systems offer the necessary security mechanisms to prevent cyberattacks? What about the malicious use of the data to serve the interests of non-democratic governments or organised crime? The truth is that it is very hard to provide an unequivocal answer to these questions. One significant challenge that our knowledge of such novel technologies is limited and will likely soon be outdated -- or turn out to be just plain wrong.

The ethical principles and standards of governance for data-driven initiatives for public good need to be clearly defined and meticulously complied with. In the past decade, numerous ethical guidelines and principles in the context of data-driven decision-making for public good, and more generally on the use of Artificial Intelligence, have been proposed. To name a few: the principles of the Menlo Report;[36] the report by the European Commission for the development of Trustworthy Artificial Intelligence;[37] the OECD[38] principles for the development of Artificial Intelligence; the ethical principles included in the national Artificial Intelligence strategies of over 20 countries in the world; and the ethics in Artificial Intelligence initiatives within professional organizations, such as the IEEE[39] and the ACM.[40] Next, we group most of the previously proposed principles using the FATEN[41] acronym, which is an extension of the four basic principles of medical ethics.[42]

1 F for fairness, i.e. free of discrimination. Data-driven algorithmic decisions might discriminate if the data used to train such algorithms is biased or if the choice of algorithm or model for the problem at hand was poor. In the past year, several highly impactful cases of algorithmic discrimination have been brought to light in public good areas, such as criminal justice[43] and healthcare.[44]

2 A for autonomy, accountability and intelligence augmentation. Autonomy is a central value in Western ethics, according to which everyone should have the ability to have sovereignty over their own thoughts and actions, thus ensuring freedom of choice, thought and behaviour. These days, though, it is possible to build computational models of our desires, needs, tastes, interests, personalities and behaviour that could be – and frequently are – used to subliminally influence our decisions and behaviours, as was the case in recent electoral processes in the US and the UK.[45] Thus, we should ensure that data-driven decision-making systems always respect human autonomy and dignity. A also stands for accountability, i.e. having clarity with respect to the attribution of responsibility for the consequences of algorithmic decisions. Finally, A stands for the augmentation – rather than substitution – of human intelligence, such that these types of systems are used to support human decision-making and not to replace humans altogether. We share the view of a "Human AI" model, as previously described.

3 T for trust and transparency. Trust is a fundamental pillar in our relationships with other humans or institutions, but it is a relative concept rather than an absolute one. We typically trust someone for a specific purpose. We might trust an institution or an individual to take custody of our money, but we might not necessarily trust the same institution or individual to take care of our children, for example. Trust emerges when three conditions are met: (1) competence, i.e. the ability to carry out the committed task; (2) reliability, i.e. sustained competence over time; and (3) honesty and transparency. Hence, the T in FATEN is also for transparency.

A data-driven decision-making system is transparent when non-experts are able to observe it and easily understand it. Data-driven decision-making systems might not be transparent for at least three reasons:[46] (1) intentionally, to protect the intellectual property of the system's creators; (2) due to the digital illiteracy of their users, which prevents them from understanding how the models work; and (3) intrinsically, given that certain statistical, machine learning approaches – such as deep learning – are extremely complex and difficult to interpret.

Moreover, we need to ensure transparency not only regarding which data is being captured, shared and analysed and for what purposes, but also in which situations humans are interacting with artificial systems as opposed to with other humans.

4 E for bEneficence and equality. The principle of bEneficence refers to having the intent of doing good and maximising the positive impact in the use of data-driven decision-making algorithms with sustainability, diversity and veracity. We cannot obviate the environmental cost of technological development, particularly when it comes to Artificial Intelligence algorithms, given their need for large amounts of data to learn from and massive amounts of computation needed to process and be trained by such data. A recent study[47] found that the carbon footprint of training just one state-of-the-art deep-learning model to perform natural language processing tasks was similar to

36 Dittrich, D. and Kenneally, E. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. United States: The Department of Homeland Security

37 European Commission. 2019. Ethics guidelines for trustworthy AI. European Union.

38 OECD. 2019. OECD Principles on AI. Paris, France: OECD.

39 The Institute of Electrical and Electronics Engineers. 2017. Ethically Aligned Design. Piscataway, NJ: IEEE.

40 Association for Computing Machinery. 2018. Code of Ethics and Professional Conduct. New York, NY: ACM.

41 Oliver, N. 2019. Governance in the Era of Data-driven Decision-making Algorithms. London, UK: Women shaping Global Economic Governance-Center for Economic Policy Research Press.

42 Gillon, R. 1994. Medical ethics: four principles plus attention to scope. UK: British Medical Journal.

43 Angwin, Julia, Larson, Jeff, Mattu, Surya and Kirchner, Lauren. 2016. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. Manhattan, NY: Pro Publica

44 Ledford, Heidi. 2019. Millions of black people affected by racial bias in health-care algorithms. Berlin, Germany: Nature.

45 Gorodnichenko, Y., Pham, T., Talavera, O., 2018. Social media, sentiment and public opinions: evidence from #Brexit and #USelection. Swansea, UK: Swansea University, School of Management

46 Burrell, Jenna. 2016. How the machine 'thinks': Understanding opacity in machine learning algorithms. Newbury Park, CA: SAGE Journals.

47 Strubell, E., Ganesh, A., McCallum, A. 2019. Energy and policy considerations for deep learning in NLP. Florence, Italy: Association for Computational Linguistics

the amount of carbon dioxide that the average American emits in two years.

Diversity is also of paramount importance, from two perspectives. First, by ensuring that the teams developing data-driven algorithms for public good are diverse, which is not the case today. Diversity is needed to maximise the chances that projects will be inclusive and relevant in the communities where they will be deployed. Second, by incorporating diversity criteria into the algorithms we design, we can minimise the existence of filter bubbles and echo chamber effects,[48] which have been – at least partially – blamed for the polarisation of public opinion we see today.

Following the First Industrial Revolution, wealth meant owning capital assets, such as factories and machines. Today, one could argue that data – and more importantly, the ability to make sense of it – is the asset that generates the most wealth, leading to the data economy.

Moreover, we need to invest in efforts to ensure the veracity of the data that is and will be used for the public good. Today, we can algorithmically generate fake text, photos, videos and audio using deep neural networks (deep fakes) that are indistinguishable from real content. If we are using data to inform decisions that impact the lives of millions of people, we need to ensure that such data is indeed truthful and a reflection of the underlying reality that the models are attempting to model.

E also stands for equality. The development and wide adoption of the Internet and the World Wide Web during the Third and Fourth Industrial Revolutions has undoubtedly been key to democratising the access to information. However, the original principles of universal access to knowledge and the democratisation of technology are in danger today due to the extreme dominance of technology giants in the US (Apple, Amazon, Microsoft, Facebook and Alphabet/Google) and China (Tencent, Alibaba, Baidu), which has led to a phenomenon known as “winner takes all”. Together, these technology companies have a market value of more than 5 trillion USD and a US market share of more than 90% in Internet searches (Google), more than 70% in social networking (Facebook) and 50% in e-commerce (Amazon). This market dominance leads to data dominance. In fact, most of these technology companies are data companies that earn billions of dollars by analysing and leveraging our data. Furthermore, a large portion of the valuable human behavioural data that could be used for public good is generated and captured by the services that these technology companies offer to their customers – services that increasingly cover all aspects of our lives, including our entertainment, sports, work, health, education, transportation and travel, social connections and communication, commerce and information, and product needs.

In addition, a significant characteristic of the 21st century is the polarisation of wealth distribution. According to the latest Global Wealth Report by Credit Suisse,[49] the 100 richest people in the world are richer than the poorest 4 billion. This accumulation of wealth in the hands of very few has been at least partially attributed to technology and the so-called Fourth Industrial Revolution. With the agrarian revolution in the Neolithic and for thousands of years afterwards, ownership of land led to wealth. Following the First Industrial Revolution, wealth meant owning capital assets, such as factories and machines. Today, one could argue that data – and more importantly, the ability to make sense of it – is the asset that generates the most wealth, leading to the data economy. If we want to maximise the positive impact of this abundance of data, we should promote new models of data ownership, management, exploitation and regulation. Data sharing used for the public good could contribute both to increasing equality in the world and to better measuring existing inequalities. An interesting data sharing model from this perspective is the concept of data cooperatives, in which participants from different sectors (frequently companies) share their data to create public value, as described in Section 2.

5 **N for non-maleficence**, i.e. minimising the negative impact that could be derived from the use of the data. Within the non-maleficence principle, we highlight the use of prudence and the need to (1) maximise data security, (2) provide reliability and reproducibility guarantees and (3) always preserve people’s privacy, as explained in Section 3.2.

Once defined and agreed, the ethical principles of data sharing will need to be published, implemented and fostered in practice through appropriate standards of governance. The roles and responsibilities of each of the three actors in data sharing (companies, public institutions and people) need to be clearly stated and accepted.

48 Sadagopan, Swathi Meenakshi. 2019. Feedback loops and echo chambers: How algorithms amplify viewpoints. United States: The Conversation.

49 Shorrocks, Anthony & Hechler-Fayd’herbe, Nannette. 2019. Global Wealth Report 2019: Global wealth rises by 2.6% driven by US & China, despite trade tensions. Zurich, Switzerland: Credit Suisse

Given the multi-disciplinary nature of data-driven projects for public good, a combination of different disciplines is required, including from the social sciences and humanities. This multi-disciplinary nature adds a level of complexity regarding the governance of the projects but is potentially beneficial when it comes to the definition of, and compliance with, ethical principles since there might already be ethicists within the teams.

Moreover, external oversight bodies might be necessary to ensure that ethical principles are complied with. For this purpose, the idea of data stewards[50] has been proposed in recent years. Data stewards are individuals or groups of individuals within an organisation who are responsible for the quality and governance of data in data-driven projects that take place in their organisations, including data sharing initiatives and/or data for social good initiatives. Alternative proposals include the appointment of chief ethics officers or the creation of an external oversight ethics board – such as OPAL's CODE (described in Section 4) — which could be in charge of auditing data for social good projects to ensure that they are aligned with the pre-defined ethical principles and human values of the societies where they are developed.

Another way to ensure compliance with the ethical principles agreed upon is by using open processes and systems as much as possible, and to foster knowledge transfer. It also calls for incentivising active partnerships between academia, civil society organizations and all those who are part of the same data ecosystem. As explained in Section 2, data trusts might also be used for data governance.

In addition, understanding the cultural and social characteristics of the societies where the projects are deployed is a must. Hence, the importance of working with local institutions and the civil society of the countries where the projects take place.

In sum, any use of data for the public good by governments or not-for-profit organisations should be fully transparent, open and accountable. The results of such use must be auditable regarding its purpose, fairness and accuracy, particularly given the fact that the definition of public good is very broad.

Even when the politics are tackled, all the necessary technology to access and analyse the data is in place and clear ethical principles have been defined and are being complied with, data sharing projects for public good will fail if they do not have a sustainable financial model behind them. That's why the fourth requirement has to do with getting the economics right.

3.4. Last but not least – Get the economics right

Most initiatives involving the sharing of private data for the public good have thus far been self-funded by companies and have largely consisted of providing data and/or statistical indicators derived from such data for free. Questions inevitably arise, however, about the financial sustainability, commercial positioning and business models of these approaches—especially in relation to "for profit" solutions.

Indeed, several companies that have been at the forefront of the "data for social good" movement over the past decade, particularly telecommunication operators like Telefonica and Orange, have also invested heavily to develop their own commercial offerings as part of their data monetisation strategies. These commercial solutions, e.g. Telefonica's SmartSteps, Vodafone's Location Insights and Orange's FluxVision, provide users and clients pre-computed indicators derived from aggregate customer data, such as population density and mobility estimations. For example, a city government or a commercial group will get in touch with these entities with a need for some indicator(s). A commercial and technical discussion will ensue to determine the characteristics and cost of the dataset(s) or indicators that can be provided. Eventually, a contract is signed that stipulates a price along with payment and technical modalities such as the project timeline. In some cases, the price might be zero—when the project is for a humanitarian cause (e.g. following an earthquake), for example.

In recent years, technology companies have joined the movement of leveraging their data for purposes related to the social good, including Facebook[51] and Google[52]. In developed countries, the granularity, volume and richness of human behavioural data accumulated by technology companies is undisputed.

These companies, however, may fear and resist the development of different "for good" solutions because they could be viewed as internal commercial threats that

50 Verhulst, Steefaan G. 2018. The Three Goals and Five Functions of Data Stewards: Data Stewards: a new Role and Responsibility for an AI and Data Age. New York: NY: Medium and The Data Stewards Network.

51 https://dataforgood.fb.com/

52 https://cloud.google.com/data-solutions-for-change/

may cannibalise their existing data-driven services. Their main rational is that the existing commercial offerings already meet some of the “for good demands”—understood as providing indicators for free in some cases. But the argument fails to understand or recognise the hurdles and requirements on the path from private data to public good, as well as shifts in public opinions and regulations. First, the underlying algorithms are closed, proprietary and generally black boxes. Indeed, while calibration may be made using the latest official demographic projections, there aren’t clear guarantees regarding their scientific rigor or their compliance with strict regulations when the data is meant to be used for public good purposes.

Black box systems, for example, are currently unfit for use by National Statistical Offices, which, according to the Fundamental Principles of Official Statistics, need to be able to itemise how the statistics they provide were derived.[53] This is an important point: In their current form, these solutions will not allow official statistics to use new data sources. Second, although prices are not public, anecdotal evidence suggests that they are expensive and usually cost far more than a research university, NSO or NGO can afford. Furthermore, individuals and groups represented in the raw datasets used may have limited involvement and information about their inclusion or exclusion in such datasets, particularly when the data is aggregated and ceases to be considered personal data. Third, access is difficult, limited to those who have the means to purchase these products and to devote the effort needed to negotiate the terms of their usage. Such systems might not be appropriate in a fast-paced world that strives for near-frictionless transactions nor for smaller providers, particularly NGOs, with less resources. Finally, the range of statistical indicators is limited to what exists in these product offerings.

These limitations, and the vision of the business units behind these data-driven commercial solutions, need to be well understood to offer complementary solutions. The key is to find a value proposition for public-good projects that is complementary to, and not at odds with, these proprietary commercial products and which still allows for a viable commercial model that then supports the investment needed by businesses to create useful insights and

53 United Nations Statistics Division. 2014. Fundamental Principles of Official Statistics (A/RES/68/261 from 29 January 2014). Geneva, Switzerland: United Nations.

design bespoke solutions for the user. That may mean serving different stakeholders and market segments, providing additional indicators (such as SDG-type and/or less granular indicators), offering additional services (such as support for use in specific cases) or serving purposes and objectives that are not monetary in nature.

Moreover, as we have discussed previously in this paper, many public-good scenarios require open, transparent and explainable algorithms that can be subject to auditing and public scrutiny regarding their reliability, fairness, accuracy and reproducibility. Commercial products might not have to satisfy these conditions.

Critically, making a convincing case for such complementary initiatives requires explaining why and how these cannot address all the needs and gaps that impede access and use of private data for public good. It also requires arguing how these complementary solutions would address unmet needs, e.g. those of National Statistical Offices. In all cases, it means designing and implementing commercial positioning and business models to ensure the financial viability of the projects. One promising option is to develop a freemium model, whereby some statistical indicators would be provided for free for some high-priority, high-impact, urgent usages (e.g. natural disasters or humanitarian crises), while others – perhaps more granular — would be fee-based, with a fee structure that could be adjusted according to users and usages. This model is currently being investigated by a few telecom operators such as Sonatel. The public sector has a role to play in fostering the development and adoption of these models through a combination of fiscal incentives, use-case development and education along with the designing of helpful legislative and regulatory frameworks.

A last question is whether people should be able to sell their own data on a data market. The cases for and against such a model can be and have been argued convincingly.[54]

These considerations and possibilities are currently being reflected and tested in the OPAL project, described below.

54 Tonetti, Christopher & Kerry, Cameron F., 2019, Should consumers be able to sell their own personal data? New York, NY, The Wall Street Journal

4. An example of the way forward: OPAL

OPAL is an example of the way forward to realise the vision of a fairer, healthier, more efficient and more inclusive society thanks to data-driven decision-making processes. OPAL is short for Open Algorithms and it is a platform –in terms of both technology and governance systems and standards – to leverage the use of data collected and controlled by private companies for public-good purposes in an ethical, scalable and sustainable manner. The main design principle consists of pushing the computation to the data, rather than ever exposing or sharing that data.

OPAL falls within the question-and-answer data sharing approach previously described in the one-to-many or few-to-many models and it builds on the years of work performed by its group of founders, including several of the individuals behind the D4D and Data For Refugees (D4R) challenges. The authors of this paper are also actively involved in OPAL: Dr. Letouzé is a co-founder and Executive Director of the OPAL project whereas Dr. Oliver has collaborated since its inception through her role at the Data-Pop Alliance.

OPAL aims to provide a blueprint and toolkit for addressing the main obstacles outlined in this paper. "Data Challenges" and bilateral agreements have demonstrated the value of data for the public sector, but have also shown how costly, complex and risky (especially those that involve irreversibly sharing "anonymised" data that might be re-identified) these arrangements can be. Rising concerns over privacy, fears of growing digital divides, and criticisms about black box algorithmic decision-making constrain innovation, investment and progress from the private sector. Other obstacles such as capacity constraints and political calculus are inhibiting meaningful progress on making data truly matter for development.

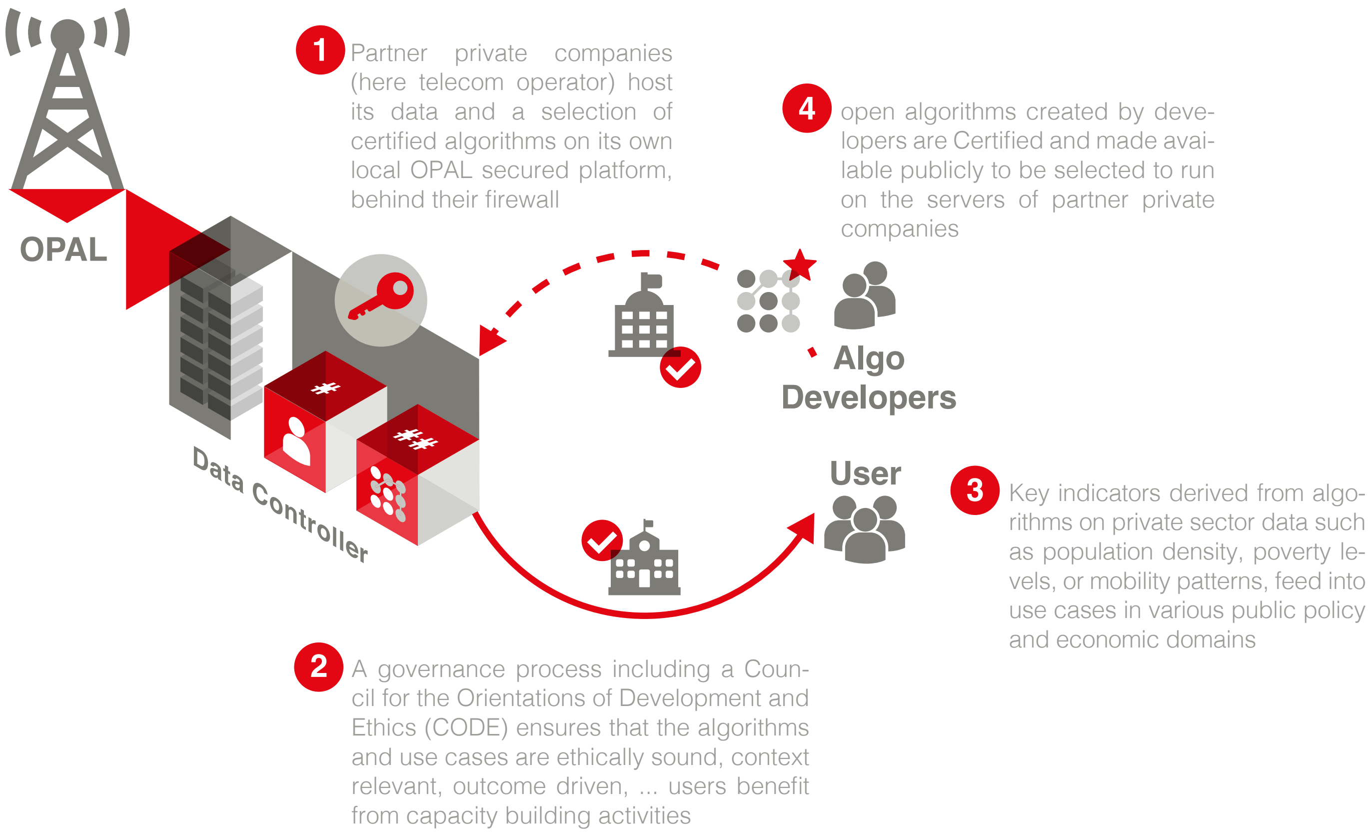
OPAL strives to change that by enabling multisector, open-source public-private federated data systems to create social value without endangering privacy and corporate value, developing appropriate systems and standards in terms of both technology and governance.

A defining feature of OPAL is its federated architecture and its question-and-answer approach, where computation is "pushed out" to the data. The data remains under the physical and custodial control of the data holder and are never shared, transferred or exposed to third parties. This federated approach can significantly reduce theft and misuse — as well as "missed use".

OPAL seeks to foster the inclusion and inputs of data subjects on the priorities and uses of analysis performed on data about them through participatory processes. Moreover, OPAL includes an oversight body called the CODE (Council for the Orientation of Development and Ethics). Sustainability is sought by strengthening local capacities and connections and by establishing viable business models. After an initial, overall successful, two-year "proof of concept" phase with pilots in Senegal and Col0mbia with telecom partners and their NSOs, OPAL is entering a "proof of market" or beta phase in both countries. The goal is to further develop and test key features and functionalities that should set OPAL on a path towards future global expansion to other telecom partners, industries, and geographies, with sustainable revenues.

OPAL is designed to be an example of how data can be at the heart of a fairer and

Figure 3: The OPAL Model



more evidence-informed approach to societal development around the globe, in the context and support of the Sustainable Development Goals (SDGs). To do so, OPAL aims to develop and deploy much-needed technological systems and governance standards addressing constraints on access and analysis of sensitive personal data collected and controlled by private organizations, allowing communities to weigh in and benefit from use cases.

OPAL's value proposition is captured by the acronym USAGE:

We believe that OPAL is one of the most promising current initiatives that can realistically provide an integrated socio-technical governance approach (i.e. a coherent set of technological and institutional systems and standards) to deliver on the promise of using sensitive personal data safely (from a privacy standpoint), ethically (especially from a local participation and oversight standpoint), and in a scalable manner (especially with its open-source approach, emphasis on capacity building, and partnerships with 2 major telecom operators) in the foreseeable future.

User-centric use cases – to show value and yield and share lessons

Algorithms: fairer, constantly updated, auditable, co-developed

Ecosystem: stronger and healthier connections between the stakeholders, built on trust

USAGE

Sales of data-driven services for public good, under a freemium model

Governance: safe data access, enabling more predictable participatory governance

5. Conclusions and Recommendations

In conclusion, we would like to offer a synthesis and some suggestions and recommendations. First, we must recognise that the issues under consideration cannot all be appropriately considered in a policy paper. They are so complex and, in part, contentious that they will only be addressed over time through processes and cycles of interactions and negotiations between stakeholders – and will thus be viewed as partial and, likely, unsatisfactory by one or more of them. It must also be noted that some major events – such as another data scandal or a major discovery—may fundamentally impact this area, on way or the other. Nevertheless, we believe that there are sound general objectives, principles and guidelines that should inform the ongoing and forthcoming interactions and negotiations that will determine how private data will be shared and used in the future – and that Europe can and should play a leading role.

In summary, let us take a look at some of our convictions we have outlined in this paper.

First, a decade into the (Big) Data Revolution, major hurdles remain, including difficulties associated with providing third parties access to these data without creating risks to individual or group privacy. In addition, there is lack of well-defined ethical principles, potential legal and regulatory barriers, technical limitations and the existence of competing commercial interests. Looking ahead, it is clear that one of the biggest questions facing all stakeholders, particularly policymakers, is whether and how these data – *or rather the insights they contain* – should be shared to maximise their potential for public-good purposes.

Next, we join other "cautious optimists" in arguing that legitimate concerns about risks must inform rather than impede attempts at making data a key force for human progress. We believe that these new kinds of crumbs and capacities have the potential to help reduce pervasive limitations in human decision-making and governance, including corruption, cognitive biases, misinformation, greed and the conflict of interests to build healthier human communities.

We furthermore believe that Europe, because of its values and assets, can lead the way in addressing those concerns, including by building on and promoting the vision behind the GDPR. We believe that data- or evidence-informed decision-support systems, where the principles and tools of machine-learning algorithms might play a central role (referred to by some authors as "Human AI" systems) can improve the state of the world by upholding rather than eroding development and democratic principles and processes.

In addition, if we are interested in the end goal—improving the world through the use of private data—we should not worry only about cracking the major first-mile problem of data access. We must instead consider the entire spectrum of hurdles and pathways that would hinder or facilitate our data crumbs to improve our communities. In short, to make data matter. We argue that this requires supporting the deployment of sustainable systems and standards, but also the development of capacities and incentives, to access, analyse and put data to use. This can only be done if we take an (eco)system perspective that does not consider data as the starting point, but which looks at how data are generated, controlled and used. The „Three Cs" framework only serves to point to systemic parts and the dynamics of these questions.

It is essential to recognise and reflect the fact that data access and sharing are only the beginning of the causal chain. Data usage and impacts must also be centrally considered. Consequently, discussions of data sharing for public good should not take place in a vacuum. They must take into account data-for-profit activities that are part of companies' efforts at monetising the data they collect and control. Whether and how privately collected and controlled data could or should be shared for the purposes of public good is not merely a technical or even a legal matter, but a complex multi-faceted one that also gets deep into political, social, ethical and business realms. Data will determine to a large extent the future of democracy and human progress. Thus, it is and will continue to be part of the structure of modern societies, a key partner to us humans, supporting our decision making.

We believe these discussions must focus on four main types of considerations: (1) political; (2) technological and scientific; (3) ethical and legal and (4) financial and commercial, within which we have identified major points and recommendations.

Politically, it is first and foremost about considering and connecting the incentives of all stakeholders in ways that balance out the long and short terms. The variety of actors (companies, public administrations and citizens) with their potentially conflicting agendas and needs must be acknowledged and actively included.

In terms of technology and science, we argue that in most cases, it is sufficient to share aggregated insights, rather than raw or pre-processed data, through technological systems that are safe and scalable as opposed to being ad hoc. We also believe that much stronger relations must be built with and within academia so as to benefit from the latest advances. Investments are essential to tackle important technical challenges, such as the lack of "ground truth" data (typically official statistics or survey data) and improve access to real-time data; the difficulties in inferring causal relationships; the complexity of combining data from multiple sources; the potential representational shortcomings of the available data, its generalisation capabilities and inherent biases; the non-existence of certification mechanisms to guarantee the quality of the algorithms applied to the data; and the lack of transparency and interpretability of complex machine-learning algorithms, such as deep neural networks.

Ethically and legally, we need to agree on and enact key ethical principles, such as the FATEN principles, with a premium not just on privacy as safety, but on privacy as agency, through participation and information, thus keeping humans and societies in the loop.

Last, we believe that using data at scale to change human systems profoundly will only be achieved if sustainable, balanced business models are in place which incentivise private actors to continue to invest in algorithms and analytics that can produce useful insights. Overall, we argue for a systemic approach to thinking and doing and we advocate for ambitious yet realistic and achievable approaches to data sharing, of which OPAL is, in our eyes, a promising example.

We formulate eight recommendations to contribute to the vision of a more just, more participatory and healthier society, one which consistently places people and their interests at its core:

1 Rather than sharing the raw data, provide secure access to actionable insights derived from the data.

2 Develop open, participatory systems and standards to enable data sharing across all companies and sectors with inputs and oversights from users, such as OPAL's code and CODE.

3 Invest ambitiously in education, capacity building, research, incentives and outreach to obtain the support and contributions from all actors private and public (including citizens) in Europe and beyond.

4 Implement incentives, remove regulatory barriers and define enabling regulations with the aim of accelerating the use of data for social good following ethical principles, such as the FATEN principles.

5 Promote corporate governance and engagement models—including the appointment of data stewards, chief ethics officers and oversight boards—that will make this area an element of standard practice in both public administrations and private companies.

6 Establish business-to-government data sharing groups in all countries and regions (see the example of Colombia or the B2G High-Level Expert Group at the European Commission).

7 Support local and regional centres of excellence that leverage private data for public good in several key cities in Europe.

8 Provide necessary funding to address the challenges mentioned above and enable a sustainable model of data sharing for public good.

We truly believe in the power of data to enable us to transition to evidence-informed societies, for and by the people. Because sharing really is caring.

Works Cited

Angwin, Julia, Larson, Jeff, Mattu, Surya and Kirchner, Lauren. 2016. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. Manhattan, NY: ProPublica.

Association for Computing Machinery. 2018. Code of Ethics and Professional Conduct. New York, NY: ACM.

Blondel, Vincent D., Decuyper, Adeline & Krings Gautier. 2015. A survey of results on mobile phone datasets analysis. Belgium: EPJ Data Sci.

Blondel, Vicent D., De Montjoye Yves-Alexandre, Hidalgo, Cesar A. & Verleysen Michel. 2013. Unique in the Crowd: The privacy bounds of human mobility. Belgium: "Communauté française de Belgique" on Information Retrieval in Time Evolving Networks.

Brockman, John, 2012. Reinventing Society in the Wake of Big Data. A conversation with Alex "Sandy" Pentland. United States: The Edge.

Brogan, Caroline. 2019. Anonymizing personal data ‚not enough to protect privacy,' shows new study. London, UK: Imperial College London.

Burrell, Jenna. 2016. How the machine 'thinks': Understanding opacity in machine learning algorithms. Newbury Park, CA: SAGE Journals.

Caraviello, Michele; Lepri, Bruno; de Oliveira, Rodrigo; Oliver, Nuria; Sebe, Nicu & Staiano, Jacopo. 2014. Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data. Seattle, WA: UbiComp 2014 - Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing.

Dwork, Cynthia and Roth, Aaron. 2014. The algorithmic foundations of differential privacy. Philadelphia, PA: University of Pennsylvania. Foundations and Trends in Theoretical Computer Science.

Dittrich, D. and Kenneally, E. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. United States: The Department of Homeland Security.

European Commission. 2018. Commission appoints Expert Group on Business-to-Government Data Sharing. European Union.

European Commission. 2019. Ethics guidelines for trustworthy AI. European Union.

Gaboardi, Marco, Honaker, James, King, Gary, Nissim, Kobbi, Ullman, Jonathan, Vadhan, Salil, and Murtagh, Jack. 2016. PSI (Ψ): a Private data Sharing Interface. New York, NY: Harvard.

García Martínez, Antonio. 2019. No, Data Is Not the New Oil. San Francisco, CA: Wired

Gillon, R. 1994. Medical ethics: four principles plus attention to scope. UK: British Medical Journal.

Gorodnichenko, Y., Pham, T., Talavera, O., 2018. Social media, sentiment and public opinions: evidence from #Brexit and #USelection. Swansea, UK: Swansea University, School of Management.

Hardinges, Jack & Wells Peter. 2018. Defining a 'data trust'. London, UK: Open Data Institute.

Hendrickx, Julien M., de Montjoye Yves-Alexandre & Rocher, Luc. 2019. Estimating the success of re-identifications in incomplete datasets using generative models. Berlin, Germany: Nature.

IDC. DOMO INC. 2018. Data Never Sleeps 6.0. American Fork, UT: DOMO.

Kolata, Gina. 2019. You Got a Brain Scan at the Hospital. Someday a Computer May Use It to Identify You. New York, NY: The New York Times.

Kolata, Gina. 2019. Your Data Were 'Anonymized'? These Scientists Can Still Identify You. New York, NY: The New York Times.

Kolbert, Elizabet. 2017. Why Facts Don't Change Our Minds. New discoveries about the human mind show the limitations of reason. New York, NY: The New Yorker.

Ledford, Heidi. 2019. Millions of black people affected by racial bias in healthcare algorithms. Berlin, Germany: Nature.

Letouzé, Emmanuel. 2012. Big Data for Development: Challenges & Opportunities. New York, NY: United Nations Publications.

Letouzé, Emmanuel, Kammourieh, Lanah & Vinck, Patrick. 2015. The Law, Politics, and Ethics of Cell Phone Data Analytics. Boston, MA: Data-Pop Alliance.

Letouzé, Emmanuel & Pentland, Alex. 2018. Towards a Human Artificial Intelligence for Human Development. ITU Journal: ICT Discoveries.

Mayer-Schönberger, Viktor & Cukier, Kenneth .2013. Big Data: A Revolution That Will Transform How We Live, Work and Think. London, UK: John Murray Publishers. ISBN 9781848547926.

OECD. 2019. OECD Principles on AI. Paris, France: OECD.

Oliver, Nuria. 2019. Governance in the Era of Data-driven Decision-making Algorithms. London, UK:Women shaping Global Economic Governance-Center for Economic Policy Research Press.

O'Neil, C. 2016. Weapons of math destruction: how big data increases inequality and threatens democracy, New York, NY: Crown, and Y. N. Harari. 2018. Why Technology Favors Tyranny. Washington, DC: The Atlantic.

Panel Secretariat led by Dr. Homi Kharas. 2013. A New Global Partnership: Eradicate poverty and transform economies through sustainable development. High-Level Panel of Eminent Persons on the Post-2015 Development Agenda. New York, NY: United Nations Publications.

Ricciato, Fabio, Lanzieri, Giampaolo & Wirthmann, Albrecht. 2019. Towards a methodological framework for estimating present population density from mobile network operator data. Luxembourg, LU: European Commission – EUROSTAT.

Sadagopan, Swathi Meenakshi. 2019. Feedback loops and echo chambers: How algorithms amplify viewpoints. United States: The Conversation.

Shorrocks, Anthony & Hechler-Fayd'herbe, Nannette. 2019. Global Wealth Report 2019: Global wealth rises by 2.6% driven by US & China, despite trade tensions. Zurich, Switzerland: Credit Suisse.

Sloane, Tim. 2019. Another Great Argument for Synthetic Data and Self-Sovereign Identity. United States: Payments Journal.

Strubell, E., Ganesh, A., McCallum, A. 2019. Energy and policy considerations for deep learning in NLP. Florence, Italy: Association for Computational Linguistics.

The Economist's Editor. 2017. The world's most valuable resource is no longer oil, but data. United States: The Economist.

The Institute of Electrical and Electronics Engineers. 2017. Ethically Aligned Design. Piscataway, NJ: IEEE.

Tonetti, Christopher & Kerry, Cameron F. 2019. Should Consumers Be Able to Sell Their Own Personal Data? New York, NY: The Wall Street Journal.

U.N. Editor. 2018. World Data Forum wraps up with a declaration to boost financing for data and statistics. New York, NY: United Nations Department of Economic and Social Affairs.

United Nations Statistics Division. 2014. Fundamental Principles of Official Statistics (A/RES/68/261 from 29 January 2014). Geneva, Switzerland: United Nations.

Verhulst, Steefaan G. 2018. The Three Goals and Five Functions of Data Stewards: Data Stewards: a new Role and Responsibility for an AI and Data Age. New York: NY: Medium and The Data Stewards Network.

Walsh, Dylan. 2019. How credit unions could help people make the most of personal data. Boston, MA: MIT Management Sloan School.

World Bank Team led by Mishra, Deepak & Deichmann, Uwe. 2016. World Development Report 2016. Digital Dividends Overview. Washington, DC: International Bank for Reconstruction and Development / The World Bank.

World Economic Forum. 2018. Our shared digital future: building an inclusive, trustworthy and sustainable digital society. Cologny/Geneva, Switzerland: World Economic Forum.

Authors

Emmanuel Letouzé, PhD

Emmanuel Letouzé is the Director and co-Founder of Data-Pop Alliance, a coalition on Big Data and development co-created in 2013 by the Harvard Humanitarian Initiative, MIT Media Lab, Overseas Development Institute, joined in 2016 by the Flowminder Foundation as its 4th core member. He is a Visiting Scholar at MIT Media Lab, a Research Affiliate at HHI and a Research Associate at ODI. He is the author of UN Global Pulse's White Paper "Big Data for Development" (2012) and of the 2013 and 2014 OECD Fragiles States reports. His research and work focus on Big Data's application and implications for official statistics, poverty and inequality, conflict, crime, and fragility, climate change, vulnerability and resilience, and human rights, ethics, and politics. He worked as a Development Economist for UNDP in New York from 2006-09 on fiscal policy, post-conflict economic recovery and migration, and between 2000-04 in Hanoi, Vietnam, for the French Ministry of Finance as a technical assistant in public finance and official statistics. He holds a BA in Political Science and an MA in Economic Demography from Sciences Po Paris, an MA from Columbia University School of International and Public Affairs, where he was a Fulbright Fellow, and a PhD from the University of California, Berkeley. He also a political cartoonist for various publications and media as 'Manu'.

Nuria Oliver, PhD

Nuria Oliver is chief data scientist at Data-Pop Alliance, chief scientific advisor at Vodafone Institute and a Fellow at the Spanish Royal Academy of Engineering. She has 20 years of research experience in human behaviour modelling, human-computer interaction and using Big Data for social good. Prior to joining Vodafone, she was Scientific Director at Telefonica R&D, the first woman to hold that position. Before that, she spent over seven years at Microsoft Research. She holds a PhD in perceptual intelligence from MIT and was named European Digital Woman of the Year in 2016 and Engineer of the Year in Spain in 2018. She holds an honorary PhD from the University Miguel Hernandez.

Her work is well known with over 150 scientific publications that have received more than 12000 citations and a ten best paper award nominations and awards. She is co-inventor of 40 filed patents and she is a regular keynote speaker at international conferences. Nuria's work and professional trajectory has received several awards, including the MIT TR100 (today TR35) Young Innovator Award (2004), the Rising Talent award by the Women's Forum for the Economy and Society (2009) and the European Digital Woman of the Year award (2016). She has been named "an outstanding female director in technology" (El PAIS, 2012), one of "100 leaders for the future" (Capital, 2009) and one of the "40 youngsters who will mark the next millennium" (El PAIS, 1999). Nuria is Board member of ELLIS.eu and OdiseIA.org.

DATA-POP ALLIANCE

Data-Pop Alliance is a global coalition on Big Data, AI and development created in 2013 by the Harvard Humanitarian Initiative, MIT Media Lab, and Overseas Development Institute, joined in 2016 by the Flowminder Foundation as its fourth core member, that brings together researchers, experts, practitioners, and activists to promote a people-centered data revolution through collaborative research, capacity and community building, and strategic design and support activities.

Vodafone Institute for Society and Communications

The institute is Vodafone's European think-tank. We analyze the potential of digital technologies and their responsible use for innovation, growth and sustainable social impact. With the help of studies and events, we offer a platform for dialogue between thought leaders from science, business and politics. Our goal is to provide better access to technology for all sections of society. The Vodafone Institute sees itself as an interdisciplinary platform and benefits from the expertise of its international advisory board.

digitising europe

With its "Digitising Europe" initiative, the Vodafone Institute provides a platform for high-level debate and exchange. Its aim is to advance a vision of a European Union in the digital age, through papers, studies, workshops, and events. This paper is part of a series of discussion papers that are focussed on challenges of European digital policy.

SHARING IS CARING
Four Key Requirements for Sustainable Private Data Sharing and Use for Public Good

Authors
Emmanuel Letouzé, PhD
Nuria Oliver, PhD

Editorial Management
Inger Paus, Managing Director, Vodafone Institute
Friedrich Pohl, Head of Communications, Vodafone Institute

Assistance
Maria Antonia Bravo,
Program Officer, Data-Pop Alliance
Luis del Carmen Garcia Rueda,
Project Operations Officer, Data-Pop Alliance

Layout
Nick Böse

Data-Pop Alliance, NYC
November 2019