

Why owning their national data is important for developing countries

Parminder Jeet Singh

There are two ways to look at the digital economy. One is just as progressive automation of production processes that has been going on for many years, now hitting a whole new level. Another is to see it as a distinct discontinuity, much like the industrial revolution was. The latter, within a few decades of some rapid techno-economic changes, begun a process that re-shaped our economic, social and political systems over the 19th and the 20th century. Though colonisation of the South had started before that, it is industrialisation that cemented it as a global economic system of extracting mineral resources from developing countries and selling them manufactured goods, making a neat profit causing continual capital accumulation.

This global economic process of North based industrial capital extracting most of the economic value has been a key factor behind geo-economic inequalities. It remained even after colonised countries gained political independence, as what has been called neo-colonisation. Over the latter part of the 20th century, global value chains increasingly got controlled through ownership of intellectual property, with much of manufacturing pushed to low cost labour centres in the South.

The deliberate invisibility of data's economic value

What is happening now is that digital capital – consisting of competencies to collect and process data, and convert it into digital intelligence – is superseding intellectual property at the top of global value chains.

Six out of eight top global firms by market cap today are digital and data driven companies, when a decade back this list was dominated by industrial giants like GE and Exxon. Not just the level of domination but also the speed at which digital and data-driven companies have achieved it are equally instructive of the power of the digital and data. Even the industrial, agriculture and IT hardware giants like, respectively, GE, Monsanto-Bayer and Intel, are declaring themselves as data-centric companies. Top automobile companies today are less afraid of competition from each other and more that Google or Apple may dominate even the transportation sector, given their digital and data skills.

Why, when every corporate boardroom seems fully focussed on the economic value of data, do policy discussions almost entirely bypass it? This subject is indeed difficult and complex, outstandingly important as it is. But perhaps more significant is the political economy behind its not being taken

up with the earnestness it requires. Northern economic and political powers – that also control much of the digital discourse through their funding and other kinds of influences over think tanks, academic research centres, etc. – are actively uninterested in discussing this issue.

The current default is that whoever collects data appropriates its entire economic value.

As they say, “possession is 90 % of law”. It is this law of the jungle that operates currently with regard to data's economic value, even as it is almost universally recognised as the central resource of the digital economy. US companies collect and process most of the world's data today and are thereby extracting billions and trillions of dollars from across the world. The EU and other OECD partners of the US have chosen to play along as faithful co-members of the rich countries club.

The North would like data's economic value to remain invisible, or (as with the EU) be clouded in narrow privacy debates. At the best, they reluctantly countenance touching upon individual ownership of data and even the very impractical idea of monetising such individual ownership. Northern scholarship has almost entirely remained confined to these areas. This has willy-nilly served to give the globally dominant digital interests time and cover to entrench their business models and economic domination globally. It would soon also convert to social, political and cultural domination. Developing countries helplessly stare at this inevitable-looking future. Scholarship and policy advocacy by civil society in the South has not been very helpful in this regard, since they too remain focussed on privacy and individual ownership of data.

Going beyond privacy and other individual data claims

It can by no stretch of logic, or pragmatism, be said that privacy is not or is less important. People's civil and political rights, and sovereignty over their personal selves and spheres, form the very basis of civilised living. But at the same time, data, and digital intelligence derived from it, are what a digital economy runs on.

The autonomously intelligent functioning of production processes and other social systems provides immense new efficiencies and benefits, just as mechanisation did for the industrial revolution.

A social and political decision must first be collectively taken as to what kinds of data should still not be produced and/or processed at all because the trade-off *vis-à-vis* possible harm may be too poor. But the decision has to be pragmatic, as per the larger public interest. For instance, it is easy to say that no location data should ever be collected, but digital transportation systems, like ride hailing services (even if of the cooperative variety), cannot run without such data. Certain kinds of ‘data denial’, or ‘all data is toxic’ pronouncements, are perhaps similar to the many poetic longings in the 19th century Europe for the pristine purity of pre-industrial life (and many such till much later in colonised countries). There is much value to such musings and literature. However, economic considerations, especially as affecting the long-term economic, political and social fate of nations, need also be able to go beyond them. Even when a ‘no collection and/or processing’ decision is taken about some kinds of data, there would still always be a lot of data – personal, social, artefactual and natural – that will need to be collected and processed, and digital intelligence extracted from it.

Economic frameworks around data need to look beyond privacy. Data is the raw product for a digital economy. The finished product is digital intelligence, which is what has real economic value.

Much of such intelligence, derived from data about people, groups and communities, is basically ‘intelligence *about* them’ – what they do, how they do it, what relationships they exist in, likelihoods of future behaviour, and so on. Unlike in the privacy framework, where it is almost like ‘you get no data about me’, people in a digital economy find that such data and ‘intelligence about them’ is useful in the hands of benign actors to get them extremely beneficial services. These can range from personal digital services – which would soon be of a digital assistant level – to all kinds of transport, health, education, livelihood, commerce, etc. related services. We already know that the overwhelming majority of people value these services immensely, and would refuse to forgo them. Indeed, if employed appropriately, these could contribute greatly to human well-being, of an order comparable to what industrialisation did.

The key digital economy issue therefore is not to entirely deny one’s data and ‘intelligence about oneself’ to anyone (although some kinds would need to be simply denied). It is to (1) share it only with trusted agents who will use such data only to one’s benefit, and (2) to remain in control of how it is used.

It is such control that can be expressed in terms of owning one’s data and ‘intelligence about oneself’.

The economic asset nature of one’s data and digital intelligence is therefore unlike physical things, or even much of intellectual property, in that the latter can entirely be

divested and separated from the original locus/creator/owner, with their economic value subsisting ‘in and of itself’. It therefore makes sense to sell physical goods or intellectual property that one may own. Data and digital intelligence about an individual or a group, however, has economic value, largely, in being applied to that particular individual or group. Meaning that its economic value can never entirely be divested from the concerned individual/group. It is therefore never wise to sell data or intelligence about oneself. The buyer of such data would simply charge that amount back to the data seller in monetary or other kinds of cost of the data-based services provided by it. The buyer would also then consider itself fully entitled to employ the resulting intelligence in all ways that suit it best, which, as per the very nature of such intelligence, is likely to be at the expense of the individual/group that initially contributed the concerned data, and about whom the data is. It can never be a beneficial bargain.

Collective or community ownership of data

What any person should therefore be really interested in is not to monetise data and digital intelligence about herself but in making sure that it is always used in a manner that is beneficial to her. The numerous initiatives about monetizing one’s data, including a recent one by the Governor of the State of California in the US, as ‘digital dividend’, are really pointless, other than to further muddy the debate about data ownership and its meaningful implementation. Even collective monetisation of data by groups and communities makes limited sense if it means that the buyer then obtains near absolute rights to use such data, and the ensuing intelligence, to control and exploit these groups and communities. Such is the kind of extreme power that data and digital intelligence puts in the hands of its owner. (Although digital companies making super profits should no doubt be adequately taxed, but that is different from collectively monetising data.)

About the real issue of being able to ensure that one’s data and digital intelligence is employed as per one’s best interests, there are two connected problems.

There is an extremely high asymmetry of power between individuals and digital corporations, and completely unrealistic expectations of personal responsibility and merit. It is practically an impossible task for individuals to undertake for themselves, and we all know this very well from experience of many years. This means that only the collective, which is strong enough to exercise its agency fruitfully, can ensure that data and digital intelligence about its members is used to their best interests, and never otherwise. This establishes the rationale for collective or community (including the national community) ownership of data and digital intelligence about the members of a given group, community or nation.

The justification for collective ownership of data is further

buttressed by a few important facts. Much of the value of data is not in individual data per se but in relationships among data of different people and groups. Such value is therefore socially located. Personal data protection is available only for personally identifiable data. But let's say there is some data about a few people living in a village, although anonymised vis-à-vis the concerned individuals separately. Such common data about what they do and how, their preferences, relationships, etc. can be used to benefit or harm them, no matter if such harm or benefit is random vis-à-vis which of these individuals actually gets harmed or benefited in any given instance.

There is no reason why these individuals as a group are not justified to together own, and control the use of, data and intelligence about them, in the same way as an individual does separately about herself.

The possible harms or benefits to people are almost as great. A group of people should therefore be able to collectively own the data about them. Further, even if not personally identifiable, many kinds of intelligence derivatives from data have huge economic value. It is logical that those whom the original data was about, and who can be considered to have contributed to its generation, have a stake in its economic value.

Many examples can be provided justifying such collective or community ownership of data. The people of a city should justifiably own the commuting data of the city, and, for instance, not have to buy it back from digital companies like Uber or Google for employing smart traffic management. Farmers should collectively own data about their fields, farm practices, local soil, climatic, etc. conditions, and not let intelligence from such data be used by digital companies to unilaterally dictate to them. And so on, practically in every sector.

Geo-economics of data

While at least the EU does make a lot of noise around data, and also around various kinds of exploitations by data companies, they prefer to see the issue from within a 'companies versus consumers' framework. This puts the entire attention on (1) privacy / personal ownership of data and (2) regulation of platforms, in which areas much work is taking place in Europe. The EU is not as interested in the geo-economic aspect of inter-country dynamics of the global digital economy, because it wants to play along with the US for retaining a Northern domination of the global economy, even as it becomes digital. (Although, internally, the EU remains very ambiguous on the issue because it is side-lined in the global data/ digital economy almost as much as the South.)

In a context where their formative digital economies are mostly born-global and remain under very strong influence if not control of US-based global corporations, developing

countries currently have very little leverage for economic self-determination in this crucial area.

For them, the most important first policy step should be to institute community (including national community) data ownership – along with policies, laws and practises arising from such a framework.

This alone will provide the economic, legal and regulatory space – or shall we say, the clay – necessary to begin shaping national digital economies that best serve the interests of their people, while maximising the unprecedented digital efficiencies and other benefits. As industrialisation required clear strong economic policies, developing countries need corresponding digital industrialisation policies for the digital era.

The dominant economic and political digital powers are most keen to pre-empt developing countries from getting wise to the need for owning their data and therefore regulating its free global flow. They are energetically inserting e-commerce chapters into various global trade agreements. At the recent World Economic Forum's annual meeting at Davos, in January 2019, they announced the launch of e-commerce negotiations at the WTO on a pluri-lateral basis. The most important objective, openly stated by its protagonists, is to ensure unrestrained and free global flow (read, appropriation) of data. While most stayed out, many developing countries have fallen prey to the lure of these negotiations, hoping that since in any case they have little grasp over the digital phenomenon, these potential agreements may help them develop their domestic digital economies and industries. The truth is exactly the opposite. These countries would be signing on to permanently attaching themselves to the losing end of global digital value chains.

Employing their data and the digital intelligence derived from it, all their sectors will be closely controlled digitally from the North, chiefly the US.

Their own people and firms would be left to do the low-end jobs of contract manufacturing, logistics, cheap local services, piece-meal digital labour like tagging pictures, some software coding, and so on, with most of the economic value being extracted to the global North. This is industrial colonisation re-visited, perhaps even worse.

Importantly, the dependency on someone who owns and controls the digital intelligence about a people – their economic, political and social activities – is so complete and abject that once caught into it, it is almost impossible for a community or nation to extract itself. The closest analogy perhaps is of a body's dependence on the brain. If the brain is controlled by external interests, there does not remain much to ever be done about it.

Exploring alternative paths

Some positive stirrings have fortunately begun to be felt among the developing countries. India recently took the first step towards a digital industrialisation strategy by instituting the concept of 'community data' in its [draft e-commerce policy](#). It has been put out for public consultations. The policy holds that communities own their data, and national data is a sovereign asset which should be employed for a country's own development. It argues the case for providing it selectively to domestic industries against allowing unrestrained access to it by foreign companies abroad. This is expected to help develop a robust domestic digital industry and economy. The policy envisions bringing out suitable legal as well as technical frameworks for these purposes.

It is hoped that other developing countries will soon begin to take similar steps, with some of them already having initiated internal discussions in this regard. Instituting community data ownership and developing the necessary legal frameworks, however, is only the right start. Developing countries will need to create a range of new data related regulatory and enabling institutions, on one hand, and many kinds of data infrastructures and community data systems and projects, on the other.

A country owning its national data does not at all mean that the state then gets a free remit on such data to control its citizens. That presents a scary picture of a data authoritarian

state, a tendency which many governments have been showing to a great extent. Neither, however, can this danger and argument be allowed to be employed to deny people, communities and nations their digital economic independence, agency and socio-economic development. This is a trap that many fall into, including in the South. Getting into a 'digital economy denial' mode will be very dangerous for the interests of people of developing countries. The historic lessons of industrialisation are once more instructive here.

What we need is some kind of a new social contract around data, expressed in data constitutionalism consisting of data related fundamental rights as well as enabling legal provisions.

Many new data related institutions are urgently needed, which are beyond the scope of this article to expand upon. Meanwhile, bringing out community data ownership and data infrastructure policies, on one hand, and instituting privacy and data protection frameworks, on the other, are two important initial steps. These should be seen as complementary and not antagonistic to one other. The [Indian draft data protection bill](#) and the community data related elements in the [draft e-commerce policy](#) highlight and express such complementarity.

Parminder Jeet Singh is a member of IT for Change, India, and of the Just Net Coalition.

This article was published in Spanish in ALAI's magazine *América Latina en Movimiento*: [Nuevas pistas de la economía mundial](#)

Digital version of this article: <https://www.alainet.org/en/articulo/198717>
