India is an emerging technology powerhouse, a significant consumer of digital services, and a treasure trove of rich and diverse digital data. While India's deliberate and dramatic digital transformation will bestow many benefits, it also creates a responsibility to pre-empt and minimise harm to consumers and citizens. As the world's largest democracy, India can chart a novel course of digital governance that leads the way even as it absorbs, emulates, and tailors global best practices to its unique context and priorities. This paper postulates that India must ensure a consumer centric approach focusing on inclusion and trust as two crucial pivots for effective digital governance and sustained digital transformation.

Digital Governanace

An Indian Perspective

Paper prepared for ICG Annual Confeence "India @75 and beyond: New Idea for The Present and Future," July2023

Key Words: *Digital Governance, Digital Transformation, Inclusion, Digital Technology, Democracy, Global South, Digital Public Infrastructure*

Dr Archana G. Gulati
Archanagg14@gmail.com

Digital Governance-An Indian Perspective

Dr Archana G. Gulati

Introduction

India is on the cusp of becoming the world's most populous and youthful economy. It is already a significant consumer of digital services, a rich and diverse digital data source, and an emerging technology powerhouse. India is likely to become a USD one trillion digital economy by 2030. (Economic Times, 2023). While India's deliberate and dramatic digital transformation will bestow many benefits, it also creates a responsibility to pre-empt and minimise harm to consumers and citizens. As the world's largest democracy, India has already been a pioneer in digital governance solutions and can chart a novel course that absorbs, emulates, and tailors global best practices to its unique context and priorities. India must ensure inclusion and consumer/citizen trust as two crucial pivots and adopt a consumer/citizen-centric approach to digital governance. This will ensure not just good governance for Indian citizens but also their sustained and transformative digital empowerment.

What is Digital Transformation

The term Digital transformation seems to have been borrowed by States and multilateral development organisations from the corporate sector. Originally it appears to have applied to commercial enterprises to signify the use of digital tools to continuously reduce user costs and improve user experience bringing about evolving and positive organisational transformation and conferring competitive advantage. (McKinsey, 2023(a)) The International Telecommunications Union (ITU) defines Digital Transformation as a journey that began at the dawn of mobile telephony and the internet and encompasses technological innovation, digitisation, and market liberalisation. It is characterised by the increasing role of information and communication technologies (ICTs) in "societies" and "economies." (ITU, 2023). It requires access, adoption, and value creation, which in turn requires other essential elements to be put in place. (Figure 1)

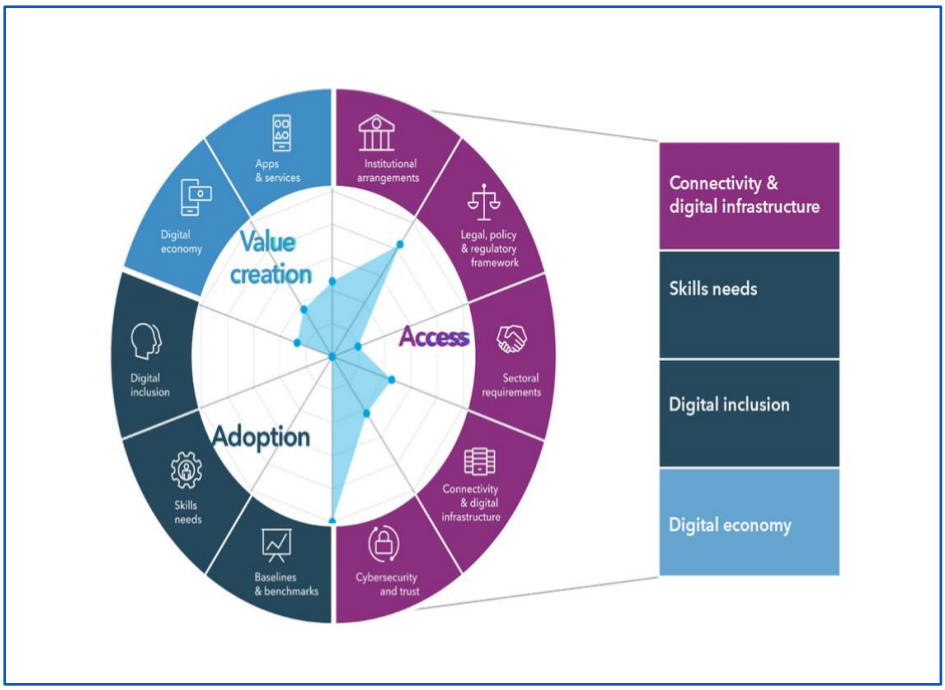


Figure 1: Digital Transformation, *Source: ITU*

What Does the Future the Look Like & for Whom?

If it is Digital Transformation that we seek, some future State (Future) must be envisioned and sought. The Future looks increasingly digital and virtual. In the times of ChatGPT, 'Singularity' or the point where the Future becomes unfathomable and unpredictable, does not appear to be so far. As Mo Gawdat explains. The march of technology is exponential and not linear. Thus, with the current technological progress of self-learning AI as the base, it is predicted that we may soon lose control over its trajectory. (Gawdat. 2021). In the wake of the global storm created by the launch of new versions of ChatGPT, leading exponents of technology have warned the world to pause and reflect before we hurtle headlong into an indeterminate future. Apart from technology and its benign and beneficial utilisation, the more significant and pressing issues relate to whom technology will serve and who will be further marginalised. Despite global efforts and phenomenal expansion in coverage, the ITU reported in September 2022 that 2.7 billion people are still to connect to the internet (ITU, 2022). Can we afford to leave anyone behind? Despite much progress in connecting millions of Indians, less than 60% of Indians are online, and in rural India, this number ranges around 30%. Going by current estimates of progress, we may not have universal internet coverage even by 2025. (Economic Times, 2023). Low mobile phone ownership among women and poor digital literacy among large sections of the population are other indicators of a digital divide that will undermine our

digital transformation agenda. We can only assume global leadership in a world moving towards augmented reality and robotics when we take everyone along. Technology and its benefits should neither be owned nor consumed by a few.

When the hitherto unconnected onboard as new users, they are especially vulnerable to online harms such as spam, cyberbullying, misinformation, and fraud. A problem surrounding fraudulent and predatory loan apps on popular play stores in India had tragic consequences for vulnerable sections of the population (Financial Express, 2021). There are many lessons to learn from this tragedy. A policymaker's response would be to improve access to safe and verified sources of credit, which is what the Government is trying to do. However, a new problem can crop up, leveraging some other gap in infrastructure or exploiting another pressing necessity. Ultimately, a combination of preventive technological solutions, due diligence and rapid responses by technology companies, and proactive consumer-centric regulation is the only way to prevent such consumer harm. In this case, while measures such as taking down apps from play stores and regulatory responses followed suit, for many hapless consumers, these came were too late.

Similarly, many examples of egregious harms from the past deployment of Artificial Intelligence (AI) prove that inclusion, transparency, and fairness from design to deployment are non-negotiable. A most infamous case is the exploitation of social media to spread AI-amplified misinformation and hatred and incite violence by bad actors in the Myanmar genocide of 2017-18. The indifferent and tardy response of the concerned technology company exacerbated the calamity. Facebook/Meta, practically synonymous with the internet in Myanmar, failed to devote the requisite attention, resources and moderate hate speech in the local language. Its conduct attracted criticism from UN Human Rights experts (Reuters, 2018). AI can amplify hate speech or be used to moderate it online. It is up to technology providers to use it responsibly and States and multilateral organisations to ensure that consumers are not collateral damage in a reckless race to profit from technology.

We know that the data used to train AI does not adequately represent several sections of the population. If this is not corrected, the foundation of this exponential technological progress will be biased, and the biases will perpetuate infinitely. How do we ensure that this time around, unlike the online harms that proliferated along with the benefits of the internet revolution, when it comes to the AI revolution or other technological progress, we can ensure that most people are much better off without making others much worse off? The foundation of the Future must

be equitable, ethical, and inclusive. This is just as important for an emerging economy like India as for any other.

Taking Stock

Before we think about the Future, we must take stock of where we stand today. India's G20 presidency has showcased our impressive progress in creating world-class digital public infrastructure (DPI) in a unique public-private partnership model. India's innovative private sector provides the technology, and the Government facilitates and provides the statutory and regulatory framework to enable mass utilisation of the DPI. A McKinsey report indicates that India has witnessed phenomenal growth in the uptake of digital services, data consumption and digital financial transactions. The report states that internet and smartphone subscribers and data consumption grew eighteenfold and screen time sevenfold in 2022 compared to 2016 ((McKinsey, 2023b).

The combination of Aadhar, the Unified Payment Interface (UPI) and the big push to spread banking coverage across the population of India has yielded rich dividends in ensuring almost universal digital financial inclusion, including even those population segments with low digital skills. In May 2023, there were 941519 million transactions on UPI, accounting for a value of Rs 14,89,14,550 crore (NPCI, 2023). UPI's success was not just because of the technology that underlies it but also the solid regulatory backup from India's financial regulator, the Reserve Bank of India, and strong support and facilitation by the Government of India. Its innovative business model riding on State-of-the-art technology is well reinforced by the trust generated by the financial regulator and the State's backing. UPI enables multiple payment applications to compete for the consumer based on quality and innovation, and the interoperable, unbundled, and decentralised yet, secure nature of its architecture makes it truly worthy of the international acknowledgement it has received. It is doubtful that multiple players could have competed so ferociously to facilitate immediate payments in India sans the UPI.

Why Consumer Trust Matters

The McKinsey report quoted above highlights that as opposed to the spurt in overall digital transactions, which grew seven-fold between 2019 and 2022, digital commerce has fared poorly and represents only seven per cent of the market. (McKinsey.2023b:19). As compared

to other nations such as Brazil or Indonesia with comparable digital penetration, Indian digital commerce lags and, starkly so. A lack of consumer 'trust' and 'comfort' have been cited as reasons for Indians, especially rural Indians, avoiding online shopping. It is essential at this juncture to point out that democratising digital commerce is expected to bring the same benefits as transacting online in another sector. It would open markets to small and medium manufacturers, suppliers and traders and give consumers access to cross-platform/marketplace/vendor price comparison and a wider choice of goods and services, thereby spurring competition and innovation.

We should ask ourselves why a consumer would shy from shopping online but not from accessing a government service or making a digital payment. The answer lies partly in practical issues such as digital skills and local language content. However, the biggest worry for consumers is the guarantee of delivery, consumer redress, and faith in the ecosystem to deliver what it promises. That the Government has repeatedly been compelled to amend the provisions relating to e-Commerce through amendments to the Foreign Direct Investment (FDI) rules and Consumer protection rules and issue rules to tackle fake reviews on e-Commerce suggests that the problem is significant and substantial. Consumers have been exploited, and large companies have used their platforms to indulge in anti-competitive practices such as self-preferencing, exploitative conduct, fake reviews, and very poor consumer redress to the detriment of third-party vendors and consumers. The other worry impacts the entire e-commerce ecosystem in India. For the same degree of interoperability and unbundling to be achieved, UPI's regulatory foundation rooted in the well-regulated Indian financial sector needs to be replicated in e-commerce; a crucial but not sole component is personal data protection and sharing.

Consumer Protection

Ensuring consumers are safe and confident about digital services is a complex problem. The foundation of digital services lies in the telecommunications network, and the same basic principles of consumer protection remain relevant regardless of how far into the Future we traverse, moving from landline telephony through mobile telephony and internet services to the realm of virtual reality, digital avatars, ubiquitous artificial intelligence or the Metaverse. The regulator of any digital service must grapple with fundamental issues of price, quality of service, inclusivity, and consumer safety. Recently, the Government has pulled up messaging apps for Unsolicited Commercial Communications, which remains a classic problem in almost

any digital communication mode ranging from voice to text to email. The Government has also warned digital players about curbing the menace of Dark Patterns, which are coercive, deceptive, or manipulative design of online interfaces that harm consumers by tricking them into making choices that benefit the online service provider at the cost of the consumer. Examples include simulating a false sense of urgency, creating hurdles in unsubscribing, nagging through repeated pop-ups etc., and "sneaking items" into the shopping baskets. (Economic Times, 2023). While clever design choices exist in the physical world too (think of the strategically located, beguiling toys/candy at the exit in an airport or mall-perfect to trigger a tired and cranky child), the scale, ease and degree of harm online are not comparable. The root of the problem lies partly in the vast troves of personal data online service providers possess about consumers, making it easy to manipulate consumer behaviour assisted ably by AI.

Thus, regulating in the digital age is far more complex and involves many distinct yet interrelated sub-areas of regulation. These include privacy and data protection, competition, and content regulation. One could look at these as the building blocks of good governance that apply regardless of whether we regulate cryptocurrency, online gaming, AI or the Metaverse.

Regulation and the Digital Consumer

The first thing to ask is who is this consumer we speak about, and why must we be consumer-centric? The simple answer is that we are all consumers. For those concerned about digital regulation, consumers include not just the average privileged individual well versed with the online world but also those yet to benefit from digital connectivity and those whose lives digital services can potentially transform. However, consumers also include those who lack digital skills or are especially vulnerable and must be protected to connect safely, sans harm.

Further, consumer concerns in a digital world differ from their brick-and-mortar counterparts. The consumer in digital markets is not just a passive recipient of goods and services. For one, digital consumers are Value Creators. If we compare the content we view on Fakebook or LinkedIn. Who is producing that value? It is the consumers themselves. In creating this value, the consumer reveals vast quantities of data and personal information apart from allowing digital players to form a very detailed picture of the individual or group of consumers' circumstances, preferences, and proclivities. The consumer is thus also a Data Subject whose personal data is the basis of behavioural marketing that keeps online services free and enables

customised content, making protecting the consumer more problematic. Yet, let us bear in mind that apart from businesses that will not continue to succeed if they harm consumers and consumers end up disenchanted with digital services; consumers are important to the State as citizens and lawmakers as voters. Consumer protection is vital on ethical grounds but also makes practical sense as a goal for every stakeholder t striving to thrive in the digital era.

Digital Transformation & Trust

Trust is a *sine qua non* for Digital Transformation. The latter is only possible if three major stakeholders, the State, industry, and consumers, trust each other. Theoretically, one could enforce or compel digital transactions, but the uptake and outcomes would be far below potential sans trust. True digital transformation also requires inclusion, a phenomenon that is much more than availability, affordability, and accessibility. Inclusion can only be authentic if consumers have the awareness and skills to utilise digital services securely and accept them as safe and trustworthy. The relationship between the two is depicted in Figure 2 below.

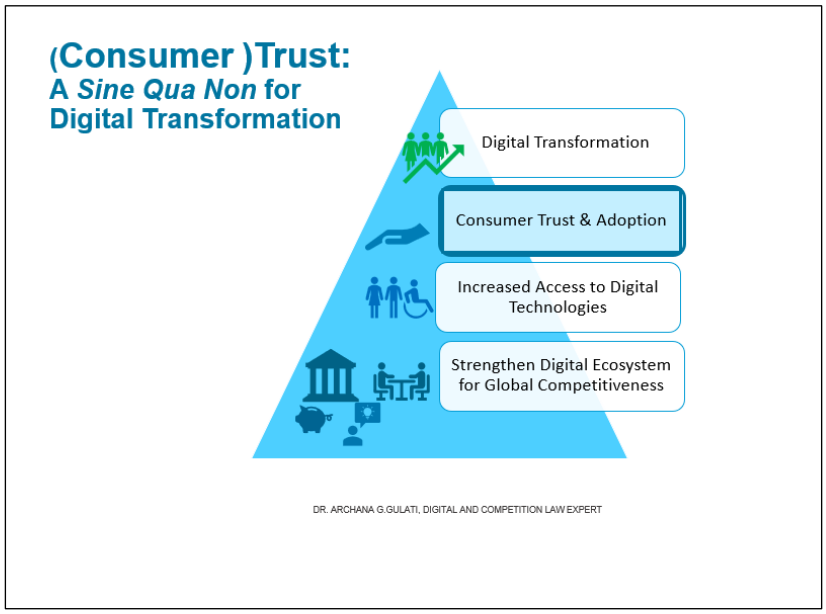


Figure 2: Digital Transformation and Trust

The resources required for Digital Transformation must come from the public and private sectors. However, a supportive and stable regulatory environment is necessary to generate a vibrant private sector that invests and innovates. Creating a conducive environment requires mutual trust between industry and the State. This trust must be built and nurtured through regulatory neutrality, transparency, fit-for-purpose regulation, and a fair and effective institutional framework to implement the rule of law.

Along with ensuring the requisite investment in digital infrastructure and its ubiquity, digital transformation demands universalisation of access. Meaningful access is much more than just availability. Even if technology & services are available and accessible, people may not be aware of how to use them, find them daunting or be reluctant to utilise them for fear of the potential harm. Without trust, adoption will be below par, and the outcomes in terms of growth and well-being will be below potential. The worst-case scenario could be a downward spiral if people reject technology, as it will impact its uptake and further investment and innovation. It has been reported that many young people in developed Western countries are switching to dumbphones to avoid the distraction and harm of smart devices (CNBC, 2023.). Perhaps, if consumers could exercise more control over being targeted by personalised content designed to hook them and keep them distracted or affect their mental health, they would not resort to such extreme measures. This has led to the development of new models of minimalistic phones- a clear example of consumers signalling and the market responding.

The other crucial aspect of trust is the relationship between the citizen and the State. In this relationship, the citizen is still a Value Creator and Data Subject in addition to being a user of public services. Given that the welfare State is the primary protector of the most vulnerable and deprived sections of the population, the responsibility of the State looms large not just as a regulator of the private digital economy but as the guardian of its citizens' digital well-being. Local language and biometrics, voice, and video-based e-governance services are a boon to less privileged or skilled and educated citizens, persons with disabilities, the elderly, rural Indians and even children. Still, consumers and data subjects repose their faith, expecting a benign and protective State. Any breach of trust in this arena is not just morally and ethically fraught; it can have far worse consequences than regulatory deficits or overkill vis-à-vis the private sector. Hence, while the State can give itself untold powers and well-meaning *carte blanche,* a lack of guard rails on its control over citizens' digital lives would have momentous consequences on Digital Transformation and empowerment, equity, and growth. On the contrary, if the State deliberately and explicitly circumscribes its power, balances it with legislation that protects citizens' moral and constitutional rights, and undertakes to create citizen awareness about these rights and mechanisms to defend these rights even against itself, the bounty in terms of Digital Transformation would be unmatched, especially in a young, emerging software strong nation like ours.

Regulation and Trust

Getting regulation right requires, first and foremost, an understanding and appreciation of the motivations of each type of stakeholder, all of whom must necessarily collaborate to ensure that digital transformation is universal, lasting, and beneficial to society. However, when incentives are not understood or appreciated, or stakeholders act purely from a short-term perspective, the result is dissonance. remedy

Digital businesses have improved our lives with innovation and valuable services. Can we imagine a world without search, email, messaging apps or e-commerce? However, it is essential for market players to actively focus on preventing consumer harm even when it seems in conflict with their profit motive because, ultimately, they will succeed only when they serve consumers and earn their trust. Similarly, regulators must create a conducive environment for investment and innovation. Yet, regulators must not hesitate to intervene to protect consumers when the industry falls short because consumer harm, mistrust and disenchantment will stand in the way of their desired growth and welfare objectives.

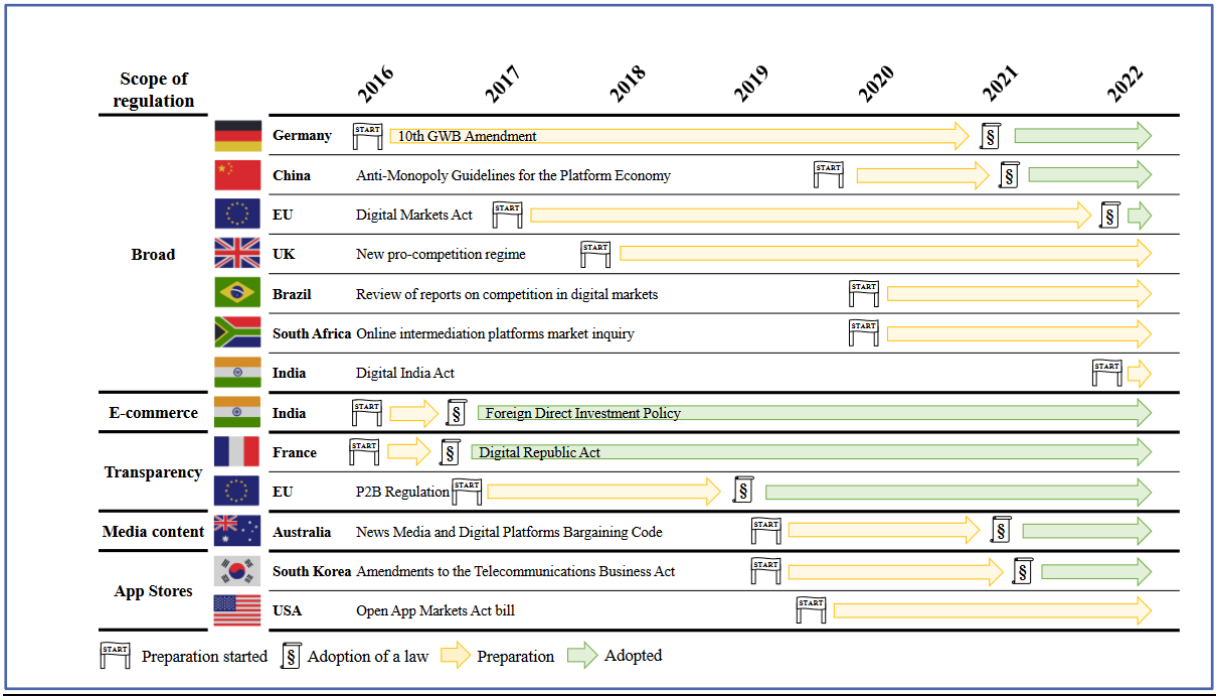
To protect consumers, the industry with the resources, information and technology must act proactively from the design stage to pre-empt harm. If harm cannot be predicted, it must be curbed. When markets are not competitive enough, as is often the case in the digital world, large and powerful market players can exploit both the poor bargaining power of consumers and competitors. They have the resources to lobby and benefit from information asymmetries as regulators catch up with new challenges from ever-evolving technology. While a detailed analysis of why this happens, especially in digital markets, is beyond the scope of this paper, suffice it to say that the current spate of regulations aimed at protecting consumers vis-à-vis competition, privacy and personal data protection and content regulation is a response to inadequate actions taken by especially more prominent players despite clear indications from their competitors, regulators, and consumers that the latter's interests are being harmed. An open dialogue between industry and regulators and mutual respect and responsiveness are essential to maintain or regain consumer safety and trust. The digital world is an excellent example of a sector where governments and regulators accepted the tremendous potential of digital goods and services to improve lives and have exercised remarkable restraint, deliberately delaying regulatory or market interventions to allow innovation to flourish. This regulatory rectitude has worked to the advantage of today's prominent players. They could have reciprocated and done more to honour the informal contract wherein they were given leeway

to self-regulate, and a particular faith was reposed in them. Had they appreciated this latitude better; we probably would not be witnessing the current global regulatory scenario. Unfortunately, what we are seeing today is the breakdown of the dialogue and the breakdown of trust. The prominent players have failed to respond quickly and with adequate measures to address consumer and competitive harms. Their responses, if any, are too little and too late, and after consumers have suffered significant harm, regulators are in overdrive to address long overdue regulatory lacunae. These gaps must be bridged, and much of the legislation is justified. However, we still run the risk of over-regulation that may do two things (A) harm innovation and (B) harm competition by inadvertently making onerous regulation an entry barrier. Regulating *ex-ante* provides (A) a speedy, specific, and effective resolution of consumer harms but runs the risk of (B) not 'getting it right,' overregulating in scope and substance, and loss of flexibility and the possibility of bespoke solutions. A principle-based regulatory approach could achieve the latter (B) but risk falling short of the former (A). (Fletcher, A. 2021),

As new regulation crops up daily in various parts of the globe, it is moot whether the digital industry could have done more and sooner. The other question is, should regulators have acted earlier, and are they overreacting now? The moral of the story is timeless. When industry and especially large market players ignore consumer harm and go too far in exploiting their market power, they bring forth harsh regulatory responses. Many would argue cynically but not entirely inaccurately that there is a demand for regulation as large firms can afford compliance and expensive litigation to keep regulators running around in circles (and lawyers in business) while ensuring that regulation becomes yet another hurdle or entry barrier for their competitors and fresh entrants respectively. Regulating the digital world is like parenting; it is hard to get it right!

If we look at regulatory responses worldwide from an industry perspective, one could blame regulators for being in overdrive mode. Figure 3 attempts to capture global regulatory responses to address the competition in digital markets. However, some caveats are often overlooked. Almost every jurisdiction has privacy & data protection regulation and has already enacted/notified or is drafting legislation to prohibit anti-competitive behaviour *ex-ante (*This includes the Digital Markets Act (EU), the upcoming Digital Markets, Competition and Consumers Bill (United Kingdom) and the Indian Digital Competition Act based on the recommendations contained in the fifty-third report of the Parliamentary Standing Committee on Finance. This is accompanied by legislation to place greater responsibility on large

platforms to ensure that consumers are safe online and that market power is not used to the detriment of consumers or smaller players. Examples include the EU's Digital Services Act and India's oft-amended Intermediary Liability rules to be subsumed into an omnibus Digital India Act. The EU has marched ahead with its rights and risks-based AI Act, while the UK plans to adopt a more cautious, flexible, and principles-based approach.

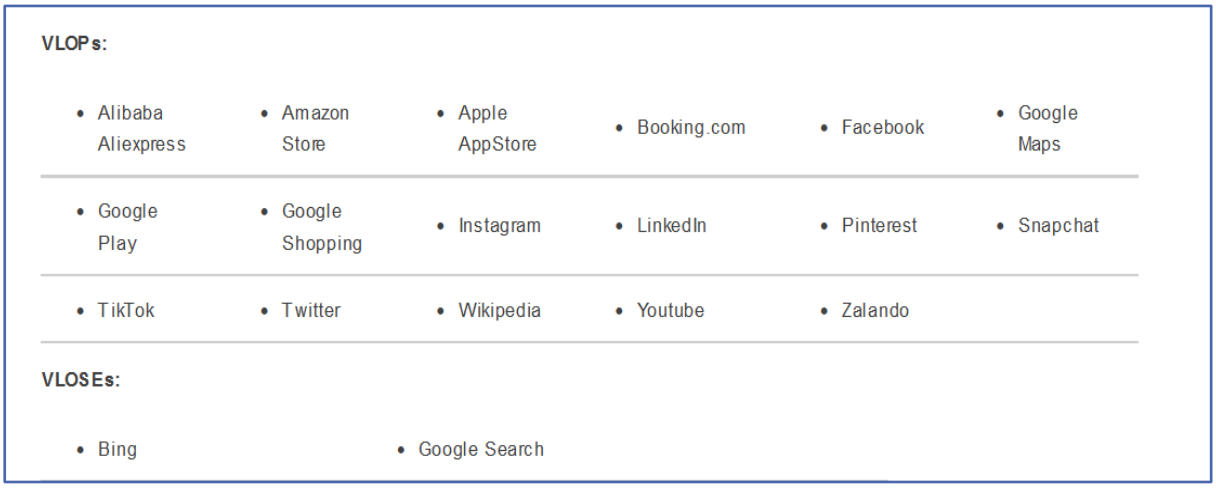


Source: Heimburg & Wiesche (2021).

Figure 3. Global Ex Ante Competition Regulations

There has been open criticism of such regulations by large technology companies and their supporters. Familiar contentions such as the adverse impact on innovation and regulatory compliance acting as an anti-competitive entry barrier are valid, even if exaggerated. Many a critic blithely ignores or is ignorant about the fact that most of the compliances in these regulations apply asymmetrically to only prominent platforms/players., For example, let us look at the DSA and DMA . Most of the regulatory compliances apply to Gatekeepers or Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), respectively (Figure 4). The Indian Parliamentary Committee also recommended ex-ante anti-competitive conduct regulation for "Systematically Important Digital Intermediaries" (SFC53,2022:31). Most Data Protection regimes have a carve-out for small and medium enterprises.

Nevertheless, it is relevant to note that all market interventions risk distorting the level playing field, and smaller firms and new entrants today would carry a heavier regulatory burden (even if lower) compared to what their gigantic counterparts faced on their entry. Thus, to the extent a piece of regulation is unnecessary, it should be avoided.



Source: European Commission

Figure 4: VLOPs & VLSOEs designated by European Commission on April 25, 2023

Thus, today's digital regulator has quite a balancing act to perform. If we look at the discussions surrounding ChatGPT, we see wildly divergent views on whether to regulate AI and how? The main concern is protecting consumers and citizens and encouraging competition and innovation. A possible solution is a regulatory response that compels the industry to act to serve the consumer without stifling innovation and competition, which brings us to another thought-provoking question.

Is Regulation the Only Solution?

Our digital world is ordered or regulated by laws, norms, architecture, and markets. An excellent example of norms is the universal priority to protect children online. Most data protection regimes do not allow their tracking of children online. Another example of norms is the type of content posted on LinkedIn instead of Meta. The relationship between governance and markets is self-evident. We probably would not binge-watch so much if Netflix charged us per episode! Therefore, markets do affect consumer behaviour. What about architecture? These are architectural issues when we speak about privacy and safety by default online. Being unable to send images and videos on regular SMS is an architectural issue. Architectural market solutions can be another way to balance bargaining power between prominent exploitative

players on one hand and consumers and smaller businesses on the other. India's DPI is precisely that type of solution.

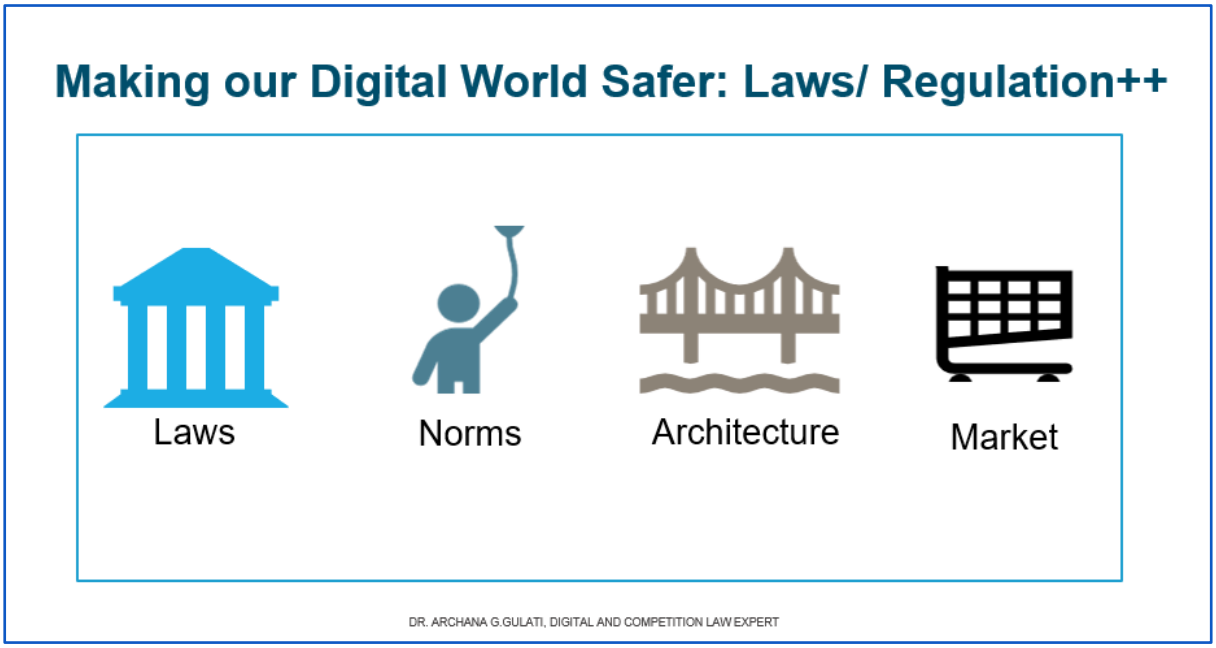


Figure 5: The Four Elements of Digital Governance

India's DPI is an excellent example of bundling all four elements of governance in a light touch, innovative, and competition-friendly solution that (when we recall the abovementioned regulator conundrums) seamlessly achieves no less than a miracle. India's Digital Public Infrastructure is interoperable, unbundled, and decentralised, a government-supported private effort, a novel public-private partnership. It has ensured competition, innovation, and, most of all, inclusion. UPI India's highly interoperable payment infrastructure has provided a common platform for multiple private players to compete based on advanced payment solutions. Without the UPI, one could imagine that the various payment systems such as banks, credit cards, and wallets would not be seamlessly interoperable and that one would not be able to make cashless payments to the smallest or remotest of online/offline sellers. It embodies the type of good innovation that spurs further innovation, competition, and the democratisation of meaningful digital access. It garners the trust of billions, and that is no mean feat.

The problem of low use of digital commerce is also sought to be addressed through an open network for digital commerce (ONDC) which will become another piece of the Indian DPI. Such a solution can rebalance the equation giving consumers and small businesses more power by design. Through ONDC, a consumer can access any number of e-commerce players, payment solutions and delivery partners on one platform and compare prices, products, and

services. Moreover, consumers can choose the payment and delivery partner without being locked into any in-house apps. Small sellers and traders can onboard quickly and access consumers without any strings attached. It is estimated that ONDC will bring 5-6 million MSMEs online and boost digital consumption (products and services) by more than fivefold by 2030 (TOI, 2023).

ONDC has ensured that global platforms are collaborating with it rather than innovating (local language solutions, use of AI, cloud computing) to only benefit their own ecosystem. A State supported but neutral architectural solution ensures that big technology companies come on board with a 'Join them, as you can't beat them' philosophy.

The highly successful Indian DPI experiment also flies in the face of the arguments that regulation hampers innovation. The breakup of market shares in the digital payments market points to a well-regulated sector displaying vigorous competition and popularity. DPI represents the entire quartet of governance: regulation, markets, architecture, and norms. The last is because of its underlying philosophy of inclusion and the democratisation of digital services, safety guaranteed by the State and regulators.

However, while brilliant architecture may solve problems of competition and inclusion and even bring forth innovation, these are necessary but insufficient for success. ONDC cannot succeed in the scale of UPI unless it tackles the trust problems that have kept e-commerce lagging in India. The secret sauce of UPI is the strength of financial regulation in India. We need an equivalent for e-Commerce. Without the backing of legislation to tackle trust issues, such as how data is securely or shared between different elements of the ONDC ecosystem, and demonstrated performance on this front, neither consumers nor vendors (large and small) would onboard to the desired extent. Thus, strengthening regulation and regulatory capacities is a *sine qua non* for the success of even architectural solutions like India's DPI, which can replace the need for regulation to curb monopolistic tendencies and introduce sectoral competition and innovation. Still, it cannot succeed without the requisite legal and institutional frameworks that build three-way trust between the critical stakeholders: industry, consumers, and the State.

This idea is even more critical for the Global South, a term loosely used to signify developing nations. In the context of the digital economy, these countries share one or many common

characteristics, such as relatively lower Internet penetration, per capita incomes and digital skills, regional disparities, and less experienced regulatory institutions.

Way Forward

On a lighter note, a digital crystal gazer would find that the Future will be replete with sensors and litigation. If the State and industry do not exercise the obligatory duty of care, both these developments will harm consumers. If technology harms, it cannot be trusted, which is particularly damaging in the context of citizen services. Well-meaning digital initiatives will fail to achieve their true digital empowerment and socio-economic well-being potential unless backed by a foundation of laws and rules that visibly protect citizens' rights and deliver redress. The way forward for a safe and inclusive digital future is a genuine, three-way collaboration between the key stakeholders: industry, the State and consumers, an idea that is not idealistic or romantic. Instead, it is indispensable to avoid a dystopic future. The digital world requires a voluntary curtailment of powers. The democratic State must earn trust as the legitimate guardian of citizens' rights, a duty it must discharge solemnly. Industry players must eschew enticing but unscrupulous uses of technology, and consumers must collectively boycott irresponsible uses of technology and its patrons.

India has already charted a unique path and can be a world leader not just in technology and its applications, as demonstrated by the DPI or the India Stack but also in global best practices that integrate deep respect for human rights, equality, diversity, and good governance by design. Our institutions are still relatively young, and given our rich tradition of democratic processes, we are uniquely poised to achieve this. By embracing such an ideal and giving it practical shape, we could differentiate ourselves from large and powerful global powers and emerge as the voice of the Global South.

References

CNBC 2023. "The rise of Dumb Phones" CNBC News.
At https://www.youtube.com/watch?v=ipGdPsYHxos. (January 18, 2023)

Economic Times, 2023. "Govt Asks Ecomm Companies to Refrain from Using Dark Patterns." July 2,.2023

Fletcher A.2022 "Ex Ante Regulation and Competition in Digital Markets" at https://www.youtube.com/watch?v=how99Vq_Fto (June 7, 2023)

Gawdat, M. "Scary Smart. The Future of Artificial Intelligence and How You Can Save Our World." September 2021. Kindle edition.

Heimburg V. & Wiesche M. 2023. "*Digital platform regulation: opportunities for information systems research"* TU Dortmund University, Dortmund, Germany April 11, 2023. At https://www.emerald.com/insight/content/doi/10.1108/INTR-05-2022-0321/full/html (June 30, 2023).

ITU 2023. AI for Good Global Summit, at https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/digital-transformation-wheel.aspx.(June 8,.2023).

McKinsey, 2023b. "Democratising Digital Commerce in India." McKinsey & Company, April 2023

McKinsey, 2023a. "What is digital transformation?" June 14, 2023. At https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation (7.6.2023)

NPCI, 2023. Product Statistics at https://www.npci.org.in/what-we-do/upi/product-statistics (June 2, 2023)

SFC53, 2022. "*Anti-competitive practices by big tech companies,"* Standing Committee on Finance, (2022-2023) -Seventeenth Lok Sabha, Ministry of Corporate Affairs, fifty-third report, Lok Sabha secretariat, New Delhi, December 2022

Fifty-Third Report of the Standing Committee on Finance

TOI 2023. "ONDC may help raise Digital Consumption 5X to $340b by 2023." Times of India, April 26,.2023

Gulati, Archana Goyal (Dr)

International Regulatory & Public Policy Expert, Strategic Adviser, Professor of Practice, Visiting Faculty. Senior Indian Civil Services Officer (Retd.)

Dr Gulati is a Strategic Adviser on Digital Transformation and Regulation of Frontier Technologies. She teaches Digital and Competition Policy & Law at leading Universities and Public Policy Institutes.

A Telecom, Digital Technology, and Competition Policy & Law Expert with over 32 years of experience, **Dr Gulati was previously an Indian Civil Services officer (1989 batch) and took voluntary retirement in 2021**. Subsequently, she worked as Senior Adviser on Competition Law with Trilegal, and was Head of Public Policy at Google, India, till October 2022.

Her educational qualifications include a BA Honours in Economics from Lady Sri Ram College, Delhi University, an LLM (Telecom & IT law) from the University of Strathclyde, UK, and a **PhD. from the Indian Institute of Technology, Delhi.**

Dr Gulati is passionate about the positive and transformative power of Digital Communications and Technologies. She believes that regulation and business practices that foster Consumer Safety and Trust are essential for Technology to be universally accepted, adopted, and deliver its potential.

She has put this philosophy into practice in her various posts in the Indian Government. Most recently, these included **Advisor (Digital Communications) at the National Institute for Transforming India (NITI Aayog).** Before that, as **Senior Deputy Director-General in the Department of Telecommunications, she served as Officer on Special Duty (OSD) to the Chairperson of the Telecom Commission of India**. She has also previously been **Advisor and Head Combinations (M&A) Division** at the **Competition Commission of India,** Financial Advisor to the Vice Chairperson of India's National Disaster Management Authority and Headed Finance as **Joint Administrator Finance of the Universal Service Fund of India.**

Dr Gulati has been an expert/resource person for the **International Telecommunication Union (ITU)** since 2010. **She was Co-rapporteur of the ITU-Development sector's Study Group 1, Q6/1 (2018-21) dealing with Consumer Protection in the Digital Age**. She has represented the Asia Pacific Region as Vice-Chair of the ITU Working Group on Finance and Human Resources.