

How should India respond to the changing era of digital 'exceptionalism'?



Raushan Tara Jaswal

Published on: 04 May 2019

OUR legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here" – these are the words that marked the beginning of digital 'exceptionalism', born from the idea that internet is different and, hence, no rules should apply.

This new, radical movement had friends in high places where the biggest companies in the stock market gave support to its think-tanks and policymakers, through which the idea of free information grew exponentially with the message of a new era – "unstoppable growth, new opportunity" (Moore's Law).

However, in 2017, it turned out that the Internet was not that different, after all. It did not bring democracy but election manipulation, not free speech but fake news, not grassroots but skyscrapers.

It is now becoming clearer than ever that this era of 'digital exceptionalism' cannot last forever and is approaching its ultimate end. Governments and courts are increasingly curbing the independence of internet firms which they

had enjoyed for so long. Public opinion is growing weary of such companies and is pushing them to police themselves better and this shift continues to accelerate. While the concepts of 'privacy', 'information overload', 'surveillance', especially the idea of being completely anonymous, seem to dominate discussions that pertain to the ever-growing reach of IOT (Internet of Things) systems, they seem to be very modern notions which go hand in hand with an increase in technology.

Shaky grounds

In fact, throughout the world, digital exceptionalism is taking a back seat especially in terms of healthcare where the risks of digital medicine, particularly the use of AI in health interventions, are concerning. Continuing to argue for digital exceptionalism and failing to robustly evaluate digital health interventions presents the greatest risk for patients and health systems, as without a clear framework to differentiate efficacious digital products from commercial opportunism, companies, clinicians, and policy makers will struggle to provide the required level of evidence to realise the potential of digital medicine.

Even in the United States, the untouchability in terms of free expression, innovation and the cornerstone of internet law, Section 230 of the Communications Decency Act (CDA), 1996, has been recently curbed through the Stop Enabling Sex Traffickers Act (SESTA), 2017, and it is argued that the law would serve as a template for future efforts at internet regulation.

Digital exceptionalism is taking a back seat especially in terms of healthcare where the risks of digital medicine, particularly the use of AI in health interventions, are concerning. Continuing to argue for digital exceptionalism and failing to robustly evaluate digital health interventions presents the greatest risk for patients and health systems, as without a clear framework to differentiate efficacious digital

products from commercial opportunism, companies, clinicians, and policy makers will struggle to provide the required level of evidence to realise the potential of digital medicine.

The question that justifies the passing of similar laws under the garb of 'national-security offences' is: why should we deny victims of terrorism and their families the chance to get justice if they can trace their harms to terrorism-facilitating content that technology companies knowingly permitted be posted or shared?

Ripple effect in India

Even though these changes in digital exceptionalism are taking place in different countries, the ripple effect makes sure that India is equally affected by it. The recent EU General Data Protection Legislation (GDPR) has extraterritorial jurisdiction and seeks to protect the fundamental rights and freedoms of natural persons in the EU and, in particular, their right to the protection of personal data. The EU comprises of a single market catering at least 500 million customers, and Indian start-ups, especially those invested in deep technology and advanced technology are witnessing a growing demand in Europe which is bolstered by the EU-India Free Trade Agreement.

Flouting the rules can attract a maximum fine equivalent to 4% of an organisation's global annual revenue or €20 million, whichever is higher. A recent report has revealed that 22% of the organisations increased their privacy budgets between 5% and 15% in the past 12 months, whereas 25% more are planning to increase their budget in the same 5% and 15% range over the next 12 months. An indication that such trends are merely a coincidence is highly unlikely and pushes the need for a more robust data protection law akin to GDPR.

India – a paradigm shift in the offing

Even though India has been a laggard in data privacy rules, especially with Aadhaar remaining a bone of contention between the government and privacy advocates, the recent Supreme Court judgment (*Justice K. Puttaswamy (Retd.) vs*

Union of India) and the BN Srikrishna Committee Report, along with the draft Data Protection Bill, should be the solution to India's rising data abuse. That said, solutions to the legal gaps in privacy and data protection should be arrived at keeping in mind historical, cultural, socio-economic and jurisprudential contexts. In India, unlike many countries across the world, the right to privacy was not treated as a fundamental right until last year. It is only now that the paradigm shift will actually happen and we shall see several connected legal norms changing. Data protection is merely one aspect that would jumpstart this change.

Needless to say, the Srikrishna Report has its own set of problematic, vague suggestions (like personal data may be processed by the Government if this is considered necessary for any function of Parliament or State Legislature), which defeat the purpose of the Supreme Court judgment. However, it ensures that personal data will need to be stored on servers that are located within India and transfers will be subject to certain safeguards.

Even though these changes in digital exceptionalism are taking place in different countries, the ripple effect makes sure that India is equally affected by it. The recent EU General Data Protection Legislation (GDPR) has extraterritorial jurisdiction and seeks to protect the fundamental rights and freedoms of natural persons in the EU and, in particular, their right to the protection of personal data. The EU comprises of a single market catering at least 500 million customers, and Indian start-ups, especially those invested in deep technology and advanced technology are witnessing a growing demand in Europe which

is bolstered by the EU-India Free Trade Agreement.

The Cambridge Analytica incident triggered calls for urgent and harsh data protection measures – and since then, other sections of the Indian government have undertaken data protection initiatives, including the Reserve Bank of India's localisation mandate for payments data, the Ministry of Health and Family Welfare's draft law protecting health data, and the Ministry of Commerce's think tank to contemplate (among other things) data protection for e-commerce. Because each of these efforts is separate from the Ministry of Electronics and Information Technology's cross-sector initiative, a fragmented landscape may emerge with conflicting and unclear obligations. This could also raise compliance costs along with having to comply with different sets of procedures.

However, the ever-increasing prevalence of Aadhaar in all sectors still poses a grave threat, especially due to the recent reports that have exposed the infrastructural gaps that still prevail. While a judgment from the apex court has recently been pronounced, various ministries have already taken heed and taken data protection policy measures. As long as inter-linkages of Aadhaar keeps continuing, there is a need to reconcile the needs of the private sector in terms of innovation, the public sector in terms of upholding the fundamental rights of citizens and the interests of the general public in terms of privacy through policy measures.

The ever-increasing prevalence of Aadhaar in all sectors still poses a grave threat, especially due to the recent reports that have exposed the infrastructural gaps that still prevail. As long as inter-linkages of Aadhaar keeps continuing, there is a need to reconcile the needs of the private sector in terms of innovation, the public sector in terms of upholding the fundamental rights of citizens and the interests of the

general public in terms of privacy through policy measures.

While it is true that policy follows technology, the era of digital exceptionalism cannot be allowed to continue unfettered, at the altar of internationally recognised fundamental rights. The Srikrishna Committee while merely a step in the right direction, as a nation, we have a long way to go especially if we were to adopt similar standards such as the GDPR in the near future, (since most private IT companies in India are already GDPR compliant and do not discriminate between EU and Indian clients). This would involve an inter-sectoral approach to privacy as a prerequisite rather than an afterthought. There are various issues of privacy especially with Aadhaar that still remain in the air even after the Supreme Court judgment and there is an emerging need for a holistic and comprehensive reconciliation of already existing policy regimes, judgments and existing infrastructure.

[Raushan Tara Jaswal is a Delhi-based lawyer and an incoming LL.M candidate at the University of Cambridge.]