gp ORF

global POLICY

GP-ORF Series

DIGITAL DEBATES

CyFy Journal 2018

Edited by Samir Saran

CyFy

Durham University

WILEY-BLACKWELL

Digital Debates
CyFy Journal Volume 5 (2018)

Authors:

Amber Sinha, Amina Khairy, Anushka Kaushik, Ashwin Rangan, Christopher Martin, Justin Hemmings, K.S. Park, Laura Sallstrom, Lina Sonne, Logan Finucan, Mihir Sharma, Nehaa Chaudhari, Rajeev Mantri, Sidhant Kumar, Sidharth Deb, Smitha Krishna Prasad, Sreenidhi Srinivasan, Stephanie MacLellan, Vidisha Mishra

Editorial Team:

Arun Mohan Sukumar, Madhulika Srikumar, Meghna Chadha, Vinia Datinguinoo Mukherjee (ORF)

Inside Design:

Artlab, Chennai

Printed by:

Times Press, New Delhi

Contents

Editor's Note

Essays

EDITOR'S NOTE

Digital Unknowns

Samir Saran

The last few years have exposed faultlines in what was once considered an integrated and seamless digital realm. These cracks have origins beyond the usual suspects. The "walls" dividing cyberspace have sprung up from within liberal democracies, throwing in question their commitment to – as the cliché goes – a "free and open" internet. The United States withdrew in 2017 from the Trans-Pacific Partnership, and in the absence of its most powerful votary, the TPP's promises on interoperability and uninterrupted flows of digital information ring hollow. The European Union has enacted one of the most far-reaching regulatory impositions on the flow of data to and from the continent in the form of the General Data Protection Regulations and the murmurings around control of the flow of technology have gained traction in the past weeks.

The GDPR, some have argued, will have the consequence of "exporting" strong privacy laws to emerging economies, which are yet to craft data protection legislations. A more likely outcome is that these economies will wean themselves away from, or script exceptional standards to manage digital commerce with the EU. Of course, opposition to the further integration of digital networks has also emerged from cybersecurity regulations in China and Russia. India's own experiment with the data protection bill is promising to upend some old assumptions around doing business with the largest digital democracy.

This year's *Digital Debates* picks up the pervasive distrust with Big Tech and the reactive regimes that have sprung up. It also discusses the often-negative spillover effects of digital communities on the real at an unprecedented velocity, emphasising the need to extend solutions beyond the virtual. Stephanie MacLellan explores this confluence of offline and digital tools to mitigate the effect of disinformation on social order across national boundaries.

Rajeev Mantri's "Reassessing Received Wisdom", as promised, calls for thinking through ownership, portability and control of data more carefully – not against the background of extant theories of regulation. Specifically, he recommends reimagining competition law for the digital economy. Fittingly, KS Park, author of "Data Socialism", moves the needle and warns against over-regulating the data market or granting ownership of data to subjects if the effect is to the detriment of realising societal benefits from data sharing.

India's recent data protection framework is the country's first attempt to balance some of these competing priorities – protecting a nascent but fast-growing digital economy and the rights of a billion users. Laura Sallstrom et al. argue that the Indian iteration is "GDPR-lite" – mimicking their EU counterpart but not sucessfully. Data localisation, according to the authors, was considered and discarded by Europe since it poses economic risks. An approach they advocate India must follow—being an economic beneficiary to the incidence of cross-border data flows.

Instead of localisation, India can consider an alternative mechanism such as a data sharing agreement under the rubric of the US Cloud Act in accessing electronic information held in the US – Justin Hemmings et al. have elaborated on this workaround in "Foundations of a Potential Executive Agreement between India and the US". Finally, Sidhant Kumar writes on the day-old judgement delivered by the Indian Supreme Court holding the world's largest unique digital identity project to be constitutional. Conscious of performing a balancing act, the Supreme Court, according to the author, favoured dogged pragmatism and not ideological dogma. All of this indicates that property rights, sovereignty and virtual territoriality continue to vex the global stakehokders and are *de jeure* creating a splinternet.

The world is witnessing, therefore, comprehensive attempts by states to govern data, the infrastructure that it is hosted on, the platforms that harvest it, and even the people who use it. The recent sight of Silicon Valley CEOs making a beeline to testify and placate US Senate Committees underlines the reality that governments, whether good or bad, autocratic or democratic, are fundamentally skeptical about the social, political and economic consequences of new technologies, and will always seek to manage them.

Given this climate, it should not surprise anyone that the Indian state too has pushed - not without opposition or controversy - for data localisation. The main trigger for this proposal has been the ceaseless troubles of Indian law enforcement agencies in securing data from abroad for criminal investigation or prosecution. But the idea has easily found takers from within India's digital companies, which are keen to insulate themselves from foreign competition and create institutional architecture that can help leverage their data analytics capabilities with locally available data. Here too, the Indian state (and established players in the private sector) are pushing for certain favourable political and economic outcomes by altering the basic DNA of the internet. Time will tell whether those outcomes materialise, but the regulatory impulse is here to stay.

If regulatory decrees are to be implemented, home-grown legal and technical standards that can function as reliable and predictable metrics for businesses and digital platforms are necessary. Amber Sinha et al. drive this point home in "Reading 'Necessity' in India's New Data Protection Bill". The principle of necessity, for instance, is critical to determine if the information sought by the data fiduciary or collector is necessary for the purpose it seeks to achieve. The authors argue that while the term "necessity" is copiously used in the draft law and would be critical to its enforcement, the same principle is not well-defined in Indian jurisprudence. Anushka Kaushik reasons that technical yardsticks, specifically encryption, in the face of competing objectives of stakeholders must be the product of mutual trust and responsibility.

Securing cyberspace or safeguarding rights online is not the only prerogative of the regulator or the state in the digital economy. Governments hold the mandate of ensuring that those at the bottom of the pyramid can exercise their agency online, perhaps in ways more impactful than in the real world. As low-cost smartphones and data bring about an entire generation of first-time internet users, policymakers must strive to grant access and security in addition to rights. Lina Sonne evaluates this trend through the increasing democratisation of content production, distribution and viewership online – mobile phones have doubled up as TV screens providing entertainment on the move, bringing "primetime" to an

end. Even as local language content online increases in volume, Ashwin Rangan notes that the internet is still predominantly "English". In his contribution titled, "Breaking the Linguistic Barriers to Accessing the Internet", he identifies the challenges to achieving a truly global internet.

Motivated by increasing inclusion, governments' digitisation drives are determined to push digital payments. Sidharth Deb proposes that any such policy approach to increase adoption must be combined with promoting ecosystem integrity and building trust with end-users.

Just as we witness the internet being "weaponised" to serve different ends, we must be humble about the transformative potential of technology. The same tool of freedom can quickly turn into a tool of oppression, manifesting socio-economic inequalities found offline. Vidisha Mishra argues that while the flexibility of the gig economy may bring more women into the workforce, these platforms may not be empowering. Without addressing structural inequalities, such as the wage gap, women stand to be disproportionately affected even after transitions in the labour market. Mihir Sharma in his contribution, "A 21-Century Social Contract", believes that a new form of social protection must be designed to adequately address these labour transitions. He points out that the increasing individualisation of labour must be met with a 21st-century economy that can work for everybody. Amina Khairy further argues that education and skilling in STEM must increase offline to truly reap the benefits that the internet offers.

Crystal-gazing is seldom an advisable pursuit, especially to discern trends in technology policy, but two issues on the horizon bear mention. Efforts to craft technology restriction regimes have recently (re)gained momentum, although export controls are unlikely to have any meaningful effect in keeping "bad" technologies from "bad" actors. In most of the developing world, export controls are perceived as technology "denial" regimes, and only facilitate the creation of networks and communities that have a vested interest in suppressing democratic aspirations or destabilise digital and physical infrastructure. Creative and agile arrangements are required to tackle the problem of proliferation of malicious ICT tools: such an arrangement has to involve the concerns of the private sector, both from developing and advanced economies. While responses that will work are hard to fathom, it may be safe to suggest that they would be technological in essence and unlikely to work if they are premised on treaties or legislation.

And finally, developments in "intelligent" platforms and services throw up – with apologies to Donald Rumsfeld – two "known unknowns" and two "unknown unknowns". The first "known unknown" is the effect of AI on bias. Pundits and technocrats both acknowledge that intelligent algorithms could perpetuate bias along the lines of race, gender and class. But we do not know what causal pathways of bias will look like and whether AI will simply mirror or exacerbate existing problems.

The second "known unknown" is the geopolitical consequences of differential access to AI. It is one thing to say some states will have lethal autonomous weapons and others won't, but access to AI translates to more than just military superiority. It is also crucial to governance platforms and services. The North-South divide in technology is already grave, but will the effect of sentient machines, with their ability to disrupt supply chains, labour markets and livelihoods compound it?

The first "unknown unknown" is whether the current conversation on "ethics" in AI will eclipse a rights-based approach to developing intelligent machines. Just as the international community appears to be close to a consensus on the promotion of human rights online, the ethical "front-loading" of AI governance could well derail that conversation. Do we share universal ethics? If not, whose "ethic" does the machine represent? The developer, business or region in which it is developed?

The second "unknown unknown" is the interweaving of identity between human and machine. Reports have recently surfaced of men trying to pursue sexually laden conversations with smart assistants and even of brutalised treatment of synthetic lifelike toys. If we engage machines in any activity that involves "human" emotion, what does that make machines? More importantly, what does our engagement with them tell us about ourselves? The digital debates of today focus on how humans should govern machines – their data, infrastructure and stability. Those of tomorrow may well focus on the new identity discourse framed around our conversations with a new intelligent being albeit shaped in our image.

Digital Debates, the journal that chronicles contemporary thinking and dialogues and along with "CyFy: The India Conference on Technology, Security and Society" will continue to seek new voices, ideas, solutions and concerns.

ESSAYS

01 Reassessing Received Wisdom and Addressing Policy Challenges of the New Technology Age

Rajeev Mantri

The rising power of global technology platforms has provoked a debate in many parts of the world: should corporate giants of the new technology age be regulated differently, even broken up?

Modern competition law doctrine traces its roots to the rise of machines during the industrial revolution of the 19th century. Widespread mechanisation and manifold increase in production capacities upended the incumbent legal regimes. Dramatic technological advancements—such as the invention of steam engine and the ability to harness fossil fuels for energy—changed the relationship between capital and labour. As economies across the world embraced these technologies—they too were "new" once but it speaks to their sweeping success that today these technologies seem largely mundane—governments have had to work hard to ensure that the legal and regulatory regimes coped. New rules were written as new industries and business models evolved.

A century later, the world finds itself at a similar juncture. Digitalisation and the fourth industrial revolution are gradually seeping into every facet of human activity and industry. It began at the turn of the new millennium with the media and communications sector, the transformation of which is plain for all to see. Increasing data uptake, connected devices and increasingly 'intelligent' machines promise to bring a new wave of change to the business landscape. Are the existing legal doctrines and regulatory institutions adequate to address the emergent challenges?

India got its first modern competition law regime in 2002 with the enactment of the Competition Act by the Atal Bihari Vajpayee government. The 2002 Act replaced the Monopolies and Restrictive Trade Practices Act of 1969 — which had come into force at the peak of the infamous Licence-Permit-Quota Raj. The Indian competition doctrine is aligned with the European template in which "abuse of dominant position" is considered anti-competitive. In contrast, the US doctrine frowns upon actions that are "in restraint of trade" and thus undermine competition in a market.

As the Yale Law School's George Priest[1] has pointed out, it is the US approach that is more economically rigorous. This approach was principally formulated by the University of Chicago's Aaron Director and Robert Bork, who showed that

the key consideration in competition regulation should be increasing consumer welfare. The two luminaries of the Chicago school pioneered the idea that the size of a business alone did not determine if it was anti-competitive. This remains an intellectual triumph for that school.

Some commentators and analysts contend that the rise of the Google-Facebook duopoly in the global digital advertising market shows the failure of the incumbent competition law doctrine. It can be argued that it is anachronistic to apply the industrial era regulations in mergers and acquisitions taking place in a networked, digital world. The competition doctrines need to take cognisance of the Metcalfe's law which posits that the value of a network increases exponentially in relation to the number of users connected to it. Seen through this lens, the large acquisitions in social networking made by Facebook become suspect, as they have allowed Facebook to accrue exponentially more market power. The Herfindahl-Hirschman Index (HHI), used by regulators to measure market concentration while evaluating mergers and acquisitions, is not able to account for the power of network effects. When an innovation is truly disruptive, it ends up creating new markets altogether. HHI presupposes that a market can be properly defined and delineated, which is a debilitating weakness that can distort the true picture when HHI is applied to the technology industries in which incumbents are willing to pay premium to pre-emptively buy-out emergent disruptors in rapidly evolving markets.

India has not seen significant debate on these issues yet as the country's digital economy – though poised for a substantial growth – is still relatively small in value. India's industrial barons and policymakers have only recently begun to take notice of the power of digital technology as it moves from being a helpful addition to marketing spiel and a hobby-horse that may pay off somewhere in the distant future, to becoming the main driving force for achieving a step jump in operational efficiency, opening new distribution channels and improving customer engagement across the consumer classes.

In this backdrop, a thicket of questions arises about how India should regulate digital businesses, with many overlapping issues. For instance, the issue of data ownership and privacy is connected with the challenges of competitive markets. If the users are owners of their personal data, should they be able to move from one service to another with seamless portability as Luigi Zingales and Guy Rolnik of the University of Chicago[2] have suggested? The issue is more complicated for India because most of the dominant businesses in the digital sphere are foreign-owned subsidiaries of the global technology giants who do not store user data in India, introducing jurisdictional questions. Additionally, several Indian technology startups are funded by global private investors, who often invest in multiple companies in the same market. While governments and regulators figure out answers to these pressing questions at their own pace, intrepid innovators are racing ahead and pushing the envelope. So far, this has largely been beneficial to consumers.

There is also a section of new 'swadeshis' who view foreign control and ownership as inimical to India's interests and competition law is a lever that can be used to reign in the influence of foreign capital in tomorrow's industries. This is a short-sighted view. Both competition and India's economy would be better served by following uniform principles for regulating technology companies – whether Indian or foreign controlled. Asking for reciprocity in openness to trade and investment is a more reasonable plank. As India's digital market grows rapidly,

it is only a matter of time before Indian businesses enter global markets and take leadership positions not just in the Anglosphere where India has a natural advantage as the world's second largest English-speaking nation, but also in the non-English speaking countries. Managing language and cultural diversity is something that comes naturally to Indian businesses, long accustomed as they are to such diversity at home, and this will provide a crucial edge when going global.

The introduction of the Goods and Services Tax (GST) in July 2017 and the concomitant end to taxing transactions have removed incentives for India's industrial firms to be vertically integrated. In the digital domain, however, there remains an incentive for integration due to the benefits of consolidation and pooling of data. Given the fungibility and costless replicability of data, it is an open question if the theory of trade specialisation should apply to digital businesses the way it does to industrial businesses. That is because integration spews out even more 'raw material' of user data that creates the competitive advantage for further extending a business into a new domain in a positive feedback loop. Data is such a versatile raw material that it is as if– to offer an analogy from the industrial context–bauxite could be turned into steel, oil could transform into copper, or iron ore could be used for making zinc.

Today Amazon is expanding successfully into the advertising business, Facebook is entering e-commerce through Instagram, and South-East Asia-focused motorbike-hailing venture Go Jek is entering payments and banking. In China, Tencent has been extending itself into commerce and payments from its strong perch in messaging and entertainment and Alibaba has become a payment and financial services giant after building dominance in China's enormous e-commerce market. India's technology leaders are following the same path, with e-commerce players entering payments, and payments providers venturing into financial services and online commerce.

Thus, most of the thorny regulatory questions concerning technology can be settled by thinking through the issues relating to ownership, portability and control of data – the raw material of the fourth industrial revolution. This discussion needs to happen with requisite changes to the extant philosophy in competition law and related areas originally designed for the industrial era to suit the requirements of the new technology era. The recent work by the University of Chicago's Eric Posner, Columbia University's Suresh Naidu and E. Glen Weyl (formerly of the University of Chicago)[3] on the rise of monopsonies in labour markets – because of employer concentration caused by network effects – is a case in point of how academic research needs to reassess received wisdom in the interest of maintaining functional markets.

Every wave of innovation brings with it a set of policy challenges. The industrial revolution of the 19th century precipitated issues of monopoly and dominance and as labour became subsidiary to capital, laws were introduced to provide for worker's rights and protections. The advent of biotechnology and medical innovations brought with it new concerns in ethics, safety and clinical testing. The rules and ideas taken for granted today were invented alongside the new technologies and they helped drive mass uptake of such technologies for sustained growth. Importantly, the process for formulating these rules, much like the development of technologies themselves, was experimental and iterative. It was not an approach

that imposed wholesale curbs on new technologies or stunted their evolution by high-handed bureaucratic diktat. While it is tempting to clamp down on the novel – and this has been the impulse of the Indian state since independence – it is permissionless innovation that is necessary to nurture the new.

02 Arab Non-Digitalised Education in the Age of Digitalisation

Amina Khairy

The millennials and Generation Z of the Arab world have the same neck-wrecking posture like their counterparts all over the world. This is hardly surprising, as the millions of Arab millennials and their fellow Generation Z are surrounded by digital technology. They lead their daily lives using digital technology such as smartphones, broadband services, and social media. According to The Arab League Educational, Scientific and Cultural Organization (ALESCO), even among the 27.1 percent of illiterate Arabs there are those who are connected to the internet, watching videos or sending photos and messages.

They are indeed "digitavorous" species. But are they equipped for a future where technology transforms jobs? Are they able to acquire the type of education that will allow them to deal with an automated job market?

Not a single parliamentarian briefing request or a political party complaint or even a popular concern has been made, at least in public, regarding the current gap in digital skills in the Arab world.

Ahmed Sabry, 12 years old, is a public middle school student in Cairo. Despite the fact that he is highly dependent on his mobile phone, he has never had any IT education. Even the IT curriculum in his school is heavily outdated, teaching hardly anything more than how to switch on and off a PC, names of keyboard buttons, and the difference between hardware and software.

Ahmed says that he hates Science, as his teachers at primary school often resorted to corporal punishment. He is not interested at all in pursuing a course that has to do with numbers. He dislikes Math, and his private tutors make things worse as they resort to theoretical explanations with no exercises.

Ahmed is just one of the majority of the youth in the Arab states who are trailing behind in linking education to work. There is a shortfall in youngsters with STEM (Science, Technology, Engineering and Mathematics) education who proceed to study Sciences at university level. Moreover, there is a lack of human and non-human resources to include digital education, especially at school level; practical visions regarding the future of jobs are also absent.

It is at school where Ahmed's core ideas and understanding of the world are formed. It is not about specialising in STEM education, but rather incorporating STEM skills at school level, where in an ideal world, governments, educators,

and businesses should be working together to achieve. Governments have the responsibility of making decisions that would best serve their people. Educators are required to change, adapt, and modernise their tools to suit the needs of those who are educated. And last but not least, it is for the benefit of businesses to be involved in education, so that they would be able to recruit competent, capable graduates who have what is needed for an automated future.

According to a report, "The Future of Jobs in the Middle East" prepared by McKinsey & Company, as much as 45 percent of all jobs in the Middle East could be automated in the near future.[1] The report, launched in the World Government Summit in February 2018, points out that US$366.6 billion in wage income and 20.8 million full-time equivalent employees are associated with jobs that are already technically automatable in six Middle Eastern countries. The countries are: Egypt, Bahrain, Oman, Kuwait, Saudi Arabia, and UAE.

Yet, the Arab world is not alone in this automated future. In the US, it is expected that one million jobs will vanish by the year 2026. They have realised that technology is transforming virtually every job in every industry. They have begun preparing workers for an automated future.

According to a commentary written by Stephen Spinelli, Jr., chancellor of Thomas Jefferson University, Americans will see a million jobs disappearing in the coming few years due to a heavily automated near future. Spinelli exhorted the American public to take a closer look at what skills are needed to meet the demands of the marketplace, and find equally paid work.[2]

Spinelli argues that this does not only mean the need for unprecedented adaptability within the workforce, but it means the need for individuals, teams, and organisations changing constantly in order to be competitive and commercial enterprises. He points out that "this puts a heavy burden on the nation's colleges and universities, which must lead the way in preparing students for professions of the future – and professionals to be students of the future". He predicts that the days are gone when students would go to college for four years, then work in a single career for the rest of their lives. Students today must be prepared to change jobs every few years, create their own jobs and curate their own careers.

Careers in the Middle East are not an exception. Early signs of automation hitting hard at jobs in the Arab world have already blossomed. According to the "Future of Jobs in the Middle East" report, 57 percent of the currently employed workforce in the Arab region have not completed a high school education. The automation potential decreases by more than half (to nearly 22 percent) for employees holding a bachelor's degree or even a graduate one. It also shows that more than 60 percent of the automation is concentrated in six of 19 sectors examined, including administrative support, government, manufacturing and construction, as well as retail and wholesale trade.

Is the Arab world's education system ready for such a challenge? The answer varies from one Arab country to the other. The Arab Social Media annual report issued by Dubai School of Government in 2013 under the title, "Transforming Education in the Arab World: Breaking Barriers in the Age of Social Learning", says that the level of satisfaction of parents with technology incorporation in their children's classrooms varied from 34.4 percent among parents with children in private schools to 19.1 percent among those with children in public schools.[3]

Most public schools in the Arab countries lack a proper education, let alone one that prepares generations for an automated future. Safaa (14 years old) is a grade 9 student in a public school in Cairo. Despite the fact that she studied, took an exam, and scored an A in a subject called "Computer Science"—she says that she and her colleagues have never come across a PC or laptop at school. "Of course I know how to Google for a song or information regarding a singer for example at the cyber cafe, but other than that I never knew what the hell the Computer Science book or teacher were talking about".

Talking about a region where more than 28 percent of the population are youth ranging between 15 and 29 years old, the educational systems—public, private, or international—are expected to supply the younger generations with the appropriate educational tools that would enable them to enter a highly automated job market.

The late 1950s, '60s, and part of the '70s witnessed a renaissance in the concept of education in a number of Arab countries. The rates of school enrolment and changing attitudes towards girls' education had a positive impact on Arab societies. However, with a few exceptions in the rich Gulf countries, the situation started to deteriorate b in the mid-1970s.

According to a report by the Council on Arab World Relations with Latin America and the Caribbean, "Unfortunately, things started changing adversely over the years. In the last several decades, the Arab region somewhat was driven away from the philosophy and essence of acquiring knowledge. As a result, the Arab world was left isolated in a world that was rapidly progressing on educational grounds".[4] The report points out to the contradictory but true fact that Arab countries grew stronger and built stable economies yet missed out on progress in many ways due to one basic fact: giving enough importance to education and its constant updating in order to cope with, adapt to, and lead into the future. One of the clearest results was missing out on the advancements of the industrial age. "It should not be forgotten that all progress was made by 'importing' machinery and other technological goods from other countries. The reason was simple – Arab countries were missing out the advancement of the industrial age."

With the industrial age come the fundamentals of science, another missed opportunity for many Arab countries. With very few exceptions—such as the late Ahmed Zoweil, the Egyptian scientist who won the 1999 Nobel Prize in Chemistry for pioneering investigations of fundamental chemical reactions on the femtosecond time scale; and Egyptian Mustapha al Sayed, the internationally recognised chemist and 2016 winner of American Chemical Society's highest honour, the Priestley Medal photo, whose research is focused on two unique areas: thermal-based cancer therapy using targeted plasmatic nanoparticles and monitoring cellular processes using a combination of enhanced spectroscopic techniques, traditional biochemistry, and dark-field microscopy/spectroscopy—Arabs made minimal contributions in exploring the depths of sciences. Not only that, but both renowned Egyptian scientists excelled in the US.

From the US and other parts of the world that have managed to keep an eye on the future of work, Arabs are set to borrow techniques, study possibilities and tailor solutions according to capabilities, given the condition that political wills will last and popular pressure will awake.

Despite the fact that there is not one prescription that fits all, Stephen Spinelli's vision on how to prepare workers for an automated future is worth a profound view. He contests the essence of college degrees. "For too long, college degrees have rewarded students' proficiency in taking exams, not their readiness for a career. As a result, students are trained to recite definitions, processes and formulas, but their lack of experience in real-world application limits their effectiveness and ability to innovate within their respective fields."[5]

If this observation sounds familiar, it is because it is true not only for the US but for the Arab world, too. Spinelli argues that higher education must focus squarely on developing the skills needed by students to succeed in a rapidly evolving job market. "We must reject the false dichotomy of theory and practice. Deep thought and decisive action must be linked – this is the imperative for today's university graduate", he suggests. He notes that despite the fact that for all the jobs that will be lost to automation in the next 13 years, hundreds of millions of new jobs will be created in response to emerging economies, ageing populations and technology development. The newly created jobs in the age of automation and digitalisation need graduates who are trained to cope, adapt, innovate and excel. But what kind of education guarantees such graduates? Spinelli's answer: "Let's leave the memorising to the robots and instead develop a networked educational system that is required of a networked society". He is not referring here to Wi-Fi on campus, which is a necessity, but rather to "trans-disciplinary learning, in which students pursuing different career paths form teams, engage with companies, help identify real-world problems, and discover innovative solutions that create value for society".

Moreover, education must become flexible through partnerships with communities, governments, as well as profit and non-profit organisations. The learning process should not be limited to the four-year university education, or the following five, six, or even ten years of post-graduate education. It has to be an ongoing lifelong practice, for this is the nature of technology, a nature that is pushing the world towards a digital automated future.

The so-called Arab Spring adds a unique taste to the region's future. In a paper titled, "Future of Artificial Intelligence and Robotics: Enabling an Arab Spring", Imad Elhahjj argues that until recently, the Arab region had been mainly a consumer of technologies. (Dr Elhahjj is member of the World Economic Forum Global Future Council on AI and Robotics.) Although numerous Arab entrepreneurs had helped shape those technologies, they had to do so from outside the region. However, Elhahjj sees the situation changing with the convergence of several technologies such as connectivity, access to information, softwarisation, cloud and development in computing.[6] He cites numbers from the Institute for Economics and Peace, which show that instead of spending US$14.3 trillion on conflict as the Arab world did in 2016, every dollar should be invested in peace-building as that can lead to a $16-decline in the cost of armed conflict. He points out that the revolution that robotics and AI can bring about in the Arab region will be a welcome change as these countries have long suffered from insecurity, financial instability and unemployment.

So what should the world spend the money on? And is it only a question of money?

Large investments do not always translate directly into improved performance. And as indicated by a report issued by Strategy& in cooperation with Google

titled, “Understanding the Arab Digital Generation” –without early rigorous preparation in technical disciplines, students at the university level tend to study the humanities. This perpetuates the region’s problem of insufficient graduates in STEM (science, technology, engineering, and math). Several MENA countries have made progress in this area recently, but there is still much work to be done.[7] One is enabling quality education for all: a principle of justice that technology enables. The “Understanding the Arab Digital Generation” report points to the fact that technology offers the means to increase fair access to education for all, including citizens in remote areas. It also facilitates teaching approaches that spur critical thinking. These benefits extend to all people in the region, not just those of school age. “Technology can promote life-long learning, such as through modular e-learning programs that help citizens acquire enhanced skills – or new skills. This can help re-engage citizens in learning, particularly those who may have dropped out of the system at an early stage”.

Despite the fact that many governments in the Arab region succeeded in securing sizable investments in education technology, such as smart classroom equipment, digital learning materials, and enhanced connectivity, the results are not satisfactory. Moreover, many teachers lack the basic skills needed to lead a classroom to a digital future, where teaching methods still rely heavily on memorisation. What make things worse are the outdated curricula that consider critical thinking and innovation as unwelcome.

Today one of the key issues in the Arab world is whether or not educators in schools and colleges realise and are capable of preparing students to work well with technology or to compete with it or rather against it. The future of work and the whole new world of jobs in an age of digitalisation and automation in the Arab world should work alongside education. It is not only a question of money to finance the educational process, but rather a package of realising the need for change, the nature of the future of work, the will to adapt and finally the decision to proceed with the change.

03 Reading 'Necessity' in India's New Data Protection Bill

Amber Sinha, Nehaa Chaudhari and Smitha Krishna Prasad

Introduction

In July 2018, a committee of experts headed by Justice BN Srikrishna submitted its draft Personal Data Protection Bill[1] to the Government of India. As the bill makes its way through the government, and potentially the parliament, several questions have been raised about the enforcement of the principles laid out in it as well as in an accompanying report.[2]

One of these questions is about how the legal principle of "necessity", developed in international law and by constitutional and administrative courts in several jurisdictions, will be imported into the reading of India's data protection law. The draft bill uses the terms "necessity" and "necessary" in many different contexts and "proportionality", which is typically a counterpart of "necessity", in specific cases.

The Srikrishna committee report dwells on "necessity" in some detail as it lays out its reasoning for the provisions in the draft bill. For example, while discussing data processing obligations, the committee explains that "necessity" is used to connect the information sought by a data fiduciary with the purpose it seeks to achieve.[3] To put it simply, what is the purpose of a data fiduciary for seeking information and is that information necessary for that purpose? The committee also refers to the use of "necessary" and "reasonably necessary" in its White Paper,[4] released earlier, to explain that these terms are meant to qualify the time for which data can be stored. They are also intended to make it easier for the government to issue guidelines and court to interpret the provisions clearly.[5]

This article identifies the different uses of the concept of "necessity" in the bill and looks at the development of the legal principle of "necessity" in international law and specific jurisdictions like the European Union (EU), the United Kingdom (UK) and India. It concludes that the jurisprudence on "necessity" is extremely sparse in India and that it will be instructive to see how the data protection authority[6] and courts interpret this term in the way personal data is collected, secured and processed.

1. An examination of "necessary" in the bill

"Necessity" as an idea manifests in many different forms across the data protection bill, beginning with its preamble. The preamble invokes it on two occasions while articulating the bill's stated aims. First, the preamble recognises that protecting personal data "as an essential facet of informational privacy" is "necessary", given the fundamental right to privacy. Second, it deems "necessary" the creation of a certain kind of "collective culture" which will enable (or champion) a "free and fair digital economy", safeguard individuals' informational privacy and guarantee "'empowerment, progress and innovation".

Later, when it goes on to detail the provisions that will realise the vision of the preamble, the bill uses "necessity" at three key places – to articulate data processing obligations and duties of data fiduciaries; the grounds for processing personal data and 'proportionality' and exemptions from certain obligations under the bill.

1.1 Data processing obligations and duties of data fiduciaries

The draft bill adopts a set of eight principles,[7] currently recognised as the bedrock of strong data protection laws around the world – fair and reasonable processing, purpose limitation, collection limitation, lawful processing, notice, data quality, data storage limitation and accountability. These principles act as duties of data fiduciaries (more commonly known as data controllers) to do certain things and refrain from doing some others.

In the sections detailing four of these obligations – collection limitation, data storage limitation, notice and data quality – the draft bill uses "necessary" in many different ways. First, "necessary" is used to quantify and limit the amount of data that data fiduciaries may collect – they may not collect more data than "necessary for the purposes of processing".[8] Second, it is used to quantify and limit the amount of time for which data fiduciaries may store data – they may not store data for longer than "reasonably necessary" to achieve the purpose of processing such data, must delete personal data if such retention is unnecessary, but may store data for longer if it is "necessary" to abide by a legal obligation.[9] Third, it is used (together with "practicable") to outline the circumstances in which data fiduciaries are required to meet a heightened "notice" requirement[10] – data fiduciaries must issue notices in multiple languages "where necessary and practicable" while notifying data principals (otherwise known as data subjects) about data processing activities.[11] Fourth, it is used while highlighting certain assessments that data fiduciaries must undertake – they must periodically assess whether it is '"necessary" for them to retain personal data.[12] Similarly, they must ascertain whether a reasonable step is "necessary" to meet data quality obligations[13] based on whether an individual's personal data may be used to make decisions about them, be disclosed to others or stored in a way that it is possible to distinguish fact based personal data from opinion or assessment based personal data.[14]

1.2 Use of 'necessity' for processing

The draft bill prescribes six grounds[15] for processing personal data. These are: consent, functions of the state, compliance with law or a court order, prompt

action, employment related purposes and reasonable purposes. Except in the case of complying with the law or a court order, "necessary" is used in provisions that deal with the grounds for mandating a nexus between the act of processing and the purpose of processing data. Like in the case of data protection obligations, "necessary" may also be read as quantifying and limiting the amount of data that data fiduciaries may collect.

For example, a data fiduciary may ask for "consent" to process personal data before providing goods/services or goods/services of a certain quality. Such a condition will be valid only to the extent of personal data "necessary" to provide the goods/services in question. Likewise, the performance of a contract or the exercise of a legal right or remedy, can be made conditional to a consent to process personal data only to the extent of data "necessary" for such performance or exercise.[16]

In addition to consent, "necessary" also qualifies certain other grounds for data processing. Where personal data is to be processed for "functions of the state", its processing must be "necessary for any function of Parliament or any State Legislature".[17] Alternatively, the processing in question must be "necessary for the exercise of any function of the State authorised by law" for the state to deliver services or benefits or issue certificates, licenses or permits to the data principal.[18] Similarly, the bill allows personal data to be processed if the processing in question is 'necessary' in certain situations that require "prompt action", such as medical emergencies and natural disasters.[19] The bill also allows personal data to be processed in certain situations in which the processing in question is 'necessary' for certain employment related purposes, such as hiring or firing, employee benefits and employee attendance, in which data fiduciary employs the data principal.[20] Further, the bill allows personal data to be processed for certain specified "reasonable purposes", but the processing must be 'necessary' for these purposes.[21]

The conditions for processing certain categories of personal data, classified as sensitive personal data,[22] are slightly different. Sensitive personal data may be processed only under four situations[23], as against six for personal data, if explicit consent is obtained – for "functions of the State", to comply with the law or a court order, or when "prompt action" is required.

Further, in each of these situations data fiduciaries must meet a heightened legal standard for their processing to be legal. For example, when personal data is processed based on consent such consent must be "explicit".[24] The bill also includes the 'necessity' standard for processing sensitive personal data in order to comply with a court order, which is absent in the case of processing personal data. More importantly, the bill sets a higher standard of 'necessity' for processing sensitive personal data where such processing is for functions of the state or in cases that require prompt action. In these cases, processing must be "strictly necessary" for the purpose sought to be achieved. The "strictly necessary" standard must also be met in order to transfer certain categories of sensitive personal data outside India – that is, some kinds of information must be stored and processed only in India, unless it is "strictly necessary" to transfer them outside for immediate action or health or emergency reasons.[25]

1.3 Use of 'necessity' in exemptions

Under the bill, processing of data in the interests of the security of the state and for law enforcement purposes is prohibited unless such processing meets certain conditions. Sections 42 and 43 of the bill, dealing with such circumstances, invoke a higher standard of 'necessity' – the processing must not only be necessary but must also be "proportionate" to the purpose sought to be achieved. In both these circumstances, if the processing meets the bill's stated criteria, including that of 'necessity' and 'proportionality', it is exempt from certain obligations under the bill.

The bill does not impose the 'necessity' and 'proportionality' standard in all cases where it exempts some processing activities from certain obligations. In all other instances, including research, statistical analysis or archiving,[26] or journalism[27] it is sufficient to demonstrate that the processing was 'necessary' for the purpose sought to be achieved. The 'necessity' and 'proportionality' standard is intended to "guard against potential misuse"[28] of the exemption by the state.

1.4 Use of 'necessity' in other contexts

The bill invokes "necessity" in some other contexts as well. "Necessary" qualifies a data principal's rights under Section 25 of the bill and restricts it to certain situations which take into account the purpose of processing data. Similarly, a data principal has the right to "restrict or prevent continuing disclosure of personal data" only in certain cases, including where the disclosure may no longer be 'necessary.'[29] The bill also uses 'necessary' to impose obligations on data fiduciaries and processors to adopt "necessary steps" to keep data secure.[30] Further, when discussing cross border transfer of sensitive personal data to a particular country or international organisation, the bill requires the central government to evaluate the 'necessity' of such action.[31]

2. Legal development of the doctrine of 'necessity'

2.1 Evolution of 'necessity' in public international law

The doctrine of "necessity" has its origins in the idea of military necessity – in the context of initiation of war as well as use of force by states during war. While early codifications of this principle go back to the 1800s, it has evolved in three different tracks of international law over the years – international humanitarian law, international criminal law, and international human rights law.[32]

In general international law, "necessity" is considered part of the rules of states' obligations, and more particularly, as a defence that may be claimed in order to preclude wrongfulness of an act of state.[33] Two factors are typically considered when applying the principle, or rather in defence of "necessity": (i) 'necessity' may only be invoked if it "is the only way for the State to safeguard an essential interest against a grave and imminent peril" and "does not seriously impair an essential interest of the State or States towards which the obligation exists or of the international community as a whole" and (ii) 'necessity' cannot be used if the international obligation in question itself does not permit reliance on such a claim or if state has contributed to the situation of 'necessity'.[34]

While the ingredients of 'necessity' vary in different streams of international law, the application of the principle in the context of human rights law is most relevant for the purposes of this article. This is also considered to represent 'necessity' at its most constraining. The basic structure of the concept is: government x is prohibited from infringing interest y unless it is necessary to achieve legitimate aim z35.

To understand the principle of "necessity" in international human rights law, it is necessary to look at the Universal Declaration of Human Rights (UDHR) of 1948 and International Covenant on Civil and Political Rights (ICCPR) of 1966. The UDHR sets out the core principles of human rights and is considered the foundational document of international human rights law, while the ICCPR is the binding treaty that spells out states' obligations and commitments towards protecting these core human rights principles.

The principle of 'necessity' typically forms one part of the tests laid out to judge whether any restriction or limitation that a state imposes on human rights is permissible. To be permissible, the restriction:

1. must be lawful or provided by law;

2. must not be arbitrary;

3. must be imposed for the purpose of achieving a legitimate aim; and

4. must be necessary to achieve such legitimate aim.

Whenever a restriction or limitation is required to be "necessary", it implies that the restriction or limitation must respond to a pressing social need, must pursue a legitimate aim and must be proportionate to such aim.[36] In addition, the limitation must be based on specific grounds justifying it in the relevant article.[37] The principle of 'necessity' is also often read to mean that state shall use no more restrictive means than are required for the achievement of the purpose of the limitation.

The right to privacy has been recognised as a fundamental human right in the UDHR and the ICCPR. Article 12 of the UDHR and Article 17 of the ICCPR both read as follows:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

"2. Everyone has the right to the protection of the law against such interference or attacks."

Early discussions on the scope of Article 17 of the ICCPR have focused on the positive obligations of the state and discussed the concepts of unlawful and arbitrary interference in limited measure. The Human Rights Committee (HRC) published its General Comment[38] 16 on Article 17 of the ICCPR as early as 1988. "Unlawful interference" was read to mean that any interference with the right to privacy must be undertaken in accordance with law, which in turn must comply with the ICCPR. "Arbitrary interference" was read to provide that "even

interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances".[39] While there was no specific reference to the principles of 'necessity' and 'proportionality' in General Comment 16, the HRC has since stated that the concept of reasonableness indicates "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".[40]

In General Comment 31, which provides an explanation about the general obligations that states have under the ICCPR, the HRC provides that states must demonstrate the 'necessity' of any restrictions on the rights guaranteed under the ICCPR and "only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of rights".[41] The obligations under the ICCPR are binding upon all branches of government and all public authorities, whether at the national, regional or local levels.[42]

With the growth in digital technology and increase in communications surveillance, particularly mass surveillance, there has been an increased focus on the obligations under Article 17 of the ICCPR within the United Nations' human rights bodies and other stakeholders at an international level. In this context, reports on the right to privacy in the digital age have recognised that any limitation to the rights under Article 17 of the ICCPR must be necessary for reaching a legitimate aim, must be proportionate to the aim and be the least intrusive option available.[43] The onus will be on the state/government to prove that these requirements have been met.

2.2 Adoption of 'necessity' and 'proportionality' to limit state actions in privacy law

The standard tests of 'adequacy, necessity and proportionality' are seen in the form of the principles of reasonableness, proportionality or 'necessity' adopted by several constitutional courts across the world.[44] The 'proportionality' analysis – which typically includes a discussion on the necessity of a measure – is considered to be one of the most successful legal transplants in the second half of the twentieth century.[45]

The following sections look at the manner in which the 'necessary' and 'proportionate' principles have been incorporated in the right to privacy across a few prominent jurisdictions.

i) European Union

The use of "necessity" as a legal doctrine against which interferences with privacy must be evaluated is first encountered in the European Convention on Human Rights, 1950 (ECHR). Article 8(1) of the ECHR states:

"Everyone shall have the right to respect for his private and family life, his home and his correspondence."

Further, Article 8(2) goes on to qualify this right by setting down the grounds on which the state may interfere with an individual's right to privacy:

"There shall be no interference by a public authority with the existence of this right except such as is in accordance with the law and is necessary in a democratic

society in the interests of national security, public safety or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Along with "in accordance with the law" and the legitimate aims identified in the provision, "necessary in a democratic society" is a clearly laid down criteria for state restrictions on the right to privacy. The European Court of Human Rights (ECt.HR) in Handyside v United Kingdom[46] held the standard of "necessary in a democratic society" to be neither "synonymous with indispensable" nor does it have the "flexibility of such expressions as admissible, ordinary, useful, reasonable or desirable". In short, there must be a pressing social need to satisfy this ground. In the same case, the ECt.HR also stated that every 'formality', 'condition', 'restriction' or 'penalty' imposed must be "proportionate to the legitimate aim pursued" and that it needs to evaluated "whether the reasons given...to justify the actual measures of "interference" are relevant and sufficient".

Over the years, one or more of the three tests of 'pressing social need', 'proportionality' and 'relevant and sufficient reasons' have been applied while interpreting 'necessity'.

'**Pressing social need**'

While the court clearly suggested a lower standard than indispensability to satisfy the test of 'necessity', the use of the phrase 'pressing social need' clearly suggests a higher level of urgency, severity or immediacy that must be satisfied.[47] In Dudgeon v United Kingdom,[48] the ECt.HR dealt with a challenge against laws criminalising homosexual activity in Northern Ireland on the grounds that without reference to factors such as where the activity took place, the age of those involved or whether they had consented or were capable of giving consent, the legislation fell short of the standard of "pressing social need".[49] In a judgment that holds important interpretive lessons for Indian courts looking to applying Puttaswamy in the future, the court held that while there may be a legitimate aim,[50] the second threshold of "necessary in a democratic society" is not met as there is no pressing social need. In order to arrive at this assessment, the court took into consideration factors such as the broader views of society and lack of sufficient evidence that the measures were justified to prevent harm to those vulnerable sections of society. The identification of both context – which may evolve over time and change based on circumstances and evidence – to evaluate severity of a pressing social need or the associated harm, detriment and negative effect on society, is important in this case.

Some of the key tests for pressing social need that have been evolved by the ECt. HR are:[51]

- Is the measure seeking to address an issue which, if left unaddressed, may result in harm to or have some detrimental effect on society or a section of society?

- Is there any evidence that the measure may mitigate such harm?

- What are the broader views (societal, historic or political) of society on the issue in question?

• Have any specific views/opposition to a measure or issue expressed by society been sufficiently taken into account?

'**Proportionality**'

In S&Marper v. United Kingdom,[52] the ECt.HR looked into the retention of DNA and fingerprint samples by law enforcement and whether it was tenable under Article 8 of the ECHR. The court accepted that legitimate aim of prevention or detection of crime or disorder was being pursued but objected to the "blanket and indiscriminate nature" of the power to obtain and retain DNA samples. Some of the key factors to hold the activity disproportionate were: lack of any consideration of "the nature or gravity of the offence" or "the age of the suspected offender", lack of limitation on time of retention, lack of safeguards such as restricted rights of an acquitted individual to get their data removed and lack of a mechanism for independent review. In another case, Z v Finland,[53] the court had looked into the question of public disclosure of personal information of individual, particularly healthcare information.

According to the Article 29 Data Protection Working Party, evaluation of a proposed measure against an existing measure to meet one of the legitimate aims must be done based on evidence led explanation of why the existing measures are no longer sufficient for meeting that need.[54]

'**Relevant and sufficient reasons**'

The third test that the ECt.HR has employed complements the first two tests by looking into whether there are relevant and sufficient reasons to justify interference under Article 8 of the ECHR based on the presence of a pressing social need and/or the whether the proposed measure is proportionate. In K&T v. Finland,[55] the issue of existence of 'relevant and sufficient reasons' came up. The Finnish authorities had decided to remove two children from the care of the applicants and place them in foster care. Here, while interfering in the privacy of family in pursuance of legitimate aims, the authorities could demonstrate 'relevant and sufficient reasons' for the removal of only one child and not the other.

ii. United Kingdom

As in the case with the EU, the principles of "necessity" and "proportionality" were first introduced into the United Kingdom law with the ECHR. While privacy jurisprudence under common law goes as far back as 1604,[56] the UK courts did not follow one established principle or rule to identify violations of individual privacy. Instead, the courts adopted a case-by-case approach on the matter.[57] The standard test adopted for judicial review under the UK common law was the Wednesbury 'reasonableness' test, which looks at

(a) whether it is reasonable for the authority in question to consider a particular matter, based on their jurisdiction and then

(b) whether the decision taken by the authority is so unreasonable that no reasonable authority would have reached such a decision.[58]

In 1998, the Human Rights Act (HRA) was enacted for the purpose of incorporating the rights under the ECHR into UK law. The HRA brought with it the 'proportionality' test developed by the ECt.HR and courts in the UK have now adopted this test at least in relation to cases that fall under the HRA.

The difference in the two tests lies in the principled basis on which decisions have to be made by the courts. The 'proportionality' test is seen to offer a more rights-protective standard of review than reasonableness. The court is expressly directed to make its own evaluations on necessity, weight, and balance, rather than whether a decision is merely beyond rational justification.[59]

In R(Daly) v. Secretary of State for Justice,[60] a prisoner's rights under Article 8 of the ECHR were in question, in the context of examination of prisoners' correspondence to maintain security. Lord Steyn noted that there is a significant overlap between the reasonableness test as traditionally applied by the UK courts and the 'proportionality' test applied by the ECt.HR and that the result of application of the two tests would be the same in most cases. However, he went on to note that the standard of review is higher in the case of the 'proportionality' test. Among the specific differences he noted between the two tests were the recognition that 'proportionality' test may require the court to look into the balance which the decision maker has struck and not just address the issue of whether the decision may be considered rational or reasonable.

This test is now being adopted by the higher courts in the UK, particularly in cases where rights under the ECHR and HRA are affected.

iii. Limited use of 'necessity' in Indian constitutional jurisprudence

It is worthwhile, at this point, to delve into the nature of restrictions that the state can impose on privacy which last year's Puttaswamy judgment discussed.[61] The judgment clearly identifies the principles of informed consent and purpose limitation as central to informational privacy. However, as discussed repeatedly both during the course of the hearings and in the judgment, privacy is not absolute, like any other fundamental right. However, restrictions on the right must be reasonable in nature. In the case of section 13 of the draft bill, the restrictions on privacy in the form of denial of informed consent need to be tested against a constitutional standard. In the Puttaswamy case, the bench was not required to provide a legal test to determine the extent and scope of the right to privacy, but they do provide sufficient guidance for us to contemplate how the limits and scope of the constitutional right to privacy could be determined in future cases.

The Puttaswamy judgment clearly states that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution"[62]. By locating the right not just in Article 21 but also in the entirety of Part III, the bench clearly requires that "the drill of various Articles to which the right relates must be scrupulously followed". This means that where transgressions on privacy relate to different provisions in Part III, the different tests under those provisions will apply along with those in Article 21. For instance, where the restrictions relate to personal freedoms, the tests under Article 19 (right to freedoms) and Article 21 (right to life and liberty) will apply.

In the case of section 13 of the bill, the three tests laid down by Justice Chandrachud are most operative –

a) the existence of a "law"

b) a "legitimate State interest" and

c) the requirement of "proportionality".

The first test is already reflected in the use of the phrase 'authorised by law' in section 13 of the bill. The test under Article 21 would imply that the function of the state should not merely be authorised by law, but that the law, in both its substance and procedure must be 'fair, just and reasonable.' The next test is that of 'legitimate state interest'. In its report, the Srikrishna committee places emphasis on Justice Chandrachud's use of "allocation of resources for human development" in an illustrative list of legitimate state interests. The report claims that the ground, functions of the state, thus satisfies the legitimate state interest.[63]

It is the final test of 'proportionality' articulated by the Puttaswamy judgement which is most operative in this context. Unlike sections 42 and 43 of the bill, which include the twin tests of 'necessity' and 'proportionality', the committee has chosen to employ only one ground in section 13. 'Proportionality' is the commonly employed ground in the European jurisprudence and common law countries. As commonly understood, the 'proportionality' test consists of three parts –

(a) Is there a rational nexus between that purpose and the infringing act?

(b) Can another, less intrusive measure be used to achieve the state purpose?

(c) Finally, is the infringement of the right too great in comparison to the public purpose that is sought to be achieved?[64]

The first test is similar to the test of proximity under Article 19 of the Constitution. The test of 'necessity' in section 13 of the bill may be viewed in this context. It must be remembered that the test of 'necessity' is not limited to situations only where it may not be possible to obtain consent while providing benefits. The insufficiencies of this standard stem from the observations made in the report as well as a relatively small amount of jurisprudence on this term in Indian law. Interestingly, the Report interestingly mentions three kinds of scenarios where 'consent' is not required – where it is not appropriate, necessary or relevant for processing. The report goes on to give an example of inappropriateness. In cases where data is being gathered to provide welfare services, there is an imbalance in power between the citizen and the state. Having made that observation, the committee inexplicably arrives at a conclusion that the response to this problem is to further erode the power available to citizens by removing the need for 'consent' altogether under section 13 of the bill.[65]

There is limited jurisprudence on the standard of 'necessity' under Indian law. The Supreme Court has articulated this test as "having reasonable relation to the object the legislation has in view". In Sahara India Real Estate v. SEBI,[66] the court refers to the 'necessity' test in the Canadian jurisprudence[67] where curtailment on rights to prevent a serious risk to proper administration of justice is only permitted where reasonably alternative measures will not prevent the risk. While deliberating

interference with the right to free speech and expression, the Supreme Court relies on the 'necessity' test and identifies factors such as the extent of prejudice on rights, effect on individuals involved in the case, over-riding necessity to curb the right to report judicial proceedings conferred on the media under Article 19(1)(a) and right of the media to challenge the order.

In other jurisdictions, 'necessity' is often also synonymous with the test of narrow tailoring, i.e., the means adopted must be those that least infringe on the right of individuals. There is no requirement of 'narrow tailoring' in provisions like section 13 of the bill – that the scope of non-consensual processing must impair the right as little as possible. It is doubly unfortunate that this test does not find a place, as 'narrow tailoring' is a test well understood in Indian law, unlike 'necessity'. This means that while there is a requirement to show that processing of personal data was necessary to provide a service or benefit, there is no requirement to process data in a way that there is minimal non-consensual processing. The fear is that as long as there is a reasonable relation between processing of data and object of the function of state, state authorities and other bodies authorised by it do not need to bother with obtaining 'consent'.

Similarly, the third test of 'proportionality' is also not represented in this provision. It provides a balancing test between the abridgment of individual rights and legitimate state interest in question and requires that the first must not outweigh the second. The absence of the 'proportionality' test leaves section 13 devoid of any such consideration. Therefore, as long as the test of 'necessity' is met under this law, it need not evaluate the denial of 'consent' against the service or benefit that is being provided. It is, therefore, necessary that 'necessity' is interpreted to include the three tests articulated by the ECt.HR or emphasis is placed on comparable standards in the Indian jurisprudence, such as proximity, reasonableness and the limiting test.

3. Conclusion

The use of "necessity" in the bill echoes, in many instances, the ways in which the word is used in the EU General Data Protection Regulation. For instance, the use of 'necessity' in section 13 is clearly drawn from the language of the GDPR. However, unlike jurisdictions like the EU, Canada and South Africa which have a rich history of jurisprudence on the term, India does not have judicial guidance on how it may be interpreted. If the Srikrishna committee intended to adopt the definition of 'necessity' as articulated by the ECt.HR, it should have clearly called out the interpretation in its report which accompanied the bill. Doing so would have provided clear guidance for the data protection authority and courts on how 'necessity' ought to be construed.

sIt is also interesting that the bill refers to 'necessity' as a standard with respect to non-state actors. 'Necessity' has evolved in the constitutional law jurisprudence to govern the interference with fundamental rights of individuals. Therefore, the way it is construed in India relies heavily on the understanding of the scope and limitations of fundamental rights and how they may be curtailed. When it comes to non-state actions, the bill is not clear whether it should draw from the fundamental rights jurisprudence in India, which may only apply to vertical rights.

The use of qualifiers to 'necessity', such as 'strict' and 'reasonable', has the potential to muddle the jurisprudence. The test of 'necessity', as understood in

other jurisdictions, is a robust one but the use of a qualifier such as 'strict' in only one context may lead to an interpretation where 'non-strict necessity' is seen as a diluted standard. In this respect also, the committee disappoints by failing to provide any guidance on how they arrived at the two standards. The way in which 'necessity' is interpreted under the Personal Data Protection Bill will be instructive, for that will determine how robust the legislation is in protecting the privacy rights of individuals. It is imperative that we get it right.

04 Data Socialism

K.S. Park

Introduction

There is hardly any doubt that Artificial Intelligence (AI) holds plenty of promise. At the same time, there are concerns that the use of AI might have exclusionary effects. There are economic concerns, for one, such as those about the jobs landscape and how it will be altered, with only the companies owning AI able to flourish. There is also the apprehension that AI algorithms will be used for credit checks and information sorting that will intensify discriminatory behaviour in hiring, for example, or granting loans. The third concern is the distress that may be caused by the fact that only a few companies own and can provide such high volumes of data. This article discusses the third area of concern.

What makes AI "intelligent" is the data fed into it. What makes AI intelligent is the experience, memory and identity; just as protein molecules alone do not make up a human brain. Therefore, what makes AI more equitable will be the equitable availability of the data used to train AI. What then are the ways to make distribution of data more equitable? Interestingly, one such attempt has been the drafting of data protection laws to make data subjects the owners of the data concerning them, or at least give them ownership-like control. What is ironic is that such ownership scheme made it more difficult for personal data to be shared with one another, e.g., judicial decisions database, creating an elite class of judges who have monopoly over how the law is meted out, and eliminating the possibility of using AI to monitor and hold accountable the judicial system to make sure it works for all and not only for the few rich. Where did we go wrong?

Who owns data about oneself?

The central tenet of data protection law, "one owns data about him or her, and therefore should have control over that data" may sound good, but it is not always sustainable and compatible with respect to others' freedom of thoughts and expressions. For example, the statement, "K.S. Park is a professor" is data about this author that is known to many. That this author, K.S. Park, can control circulation of such data will be impossible in a free society, especially after he has introduced himself as a professor to countless numbers of people. When and under what grounds can this author then control perfectly lawful data that resides in another person's head, assuming it is non-defamatory and non-confidential?

The mental exercise, "one owns data about him or her" originates from the concept of "data surveillance", a term coined by Alan Westin in his 1967 book, "Privacy and Freedom"[1] . The idea is that when a person discloses data about themselves to governments and companies, the processing of such data for purposes not contemplated by the data subject or the disclosure to agencies

not thus contemplated can constitute "surveillance"—in a sense that the data controller will learn more information about the data subject than they intended to give the agency. Of course, the term "surveillance" usually means acquisition of data about another against their will, such as wiretapping, or search and seizure. But even voluntary disclosures of data can—if the conditions of the disclosures are not adhered to—lead to revealing something about oneself against one's will, and thus bringing about the term "data surveillance."

Westin, in an effort to protect people from data surveillance, proposed giving all data subjects some sort of property right on the data about them, because making promises about how the data will be used is insufficient—these promises are hard to enforce, and more importantly, powerless individuals will have a hard time bargaining those promises from the governments and companies.[2] By proposing a property right, as opposed to a contractual, the data subject's control will be a default position from which the data controller can depart only by obtaining affirmative and explicit consent from the data subjects whenever it takes the data, for the purpose and scope of data use and disclosure, just like someone borrowing a car from another will have affirmative duties to obtain consent from the car owner about its use. Westin's proposal has persuaded an increasing number of countries and people around the world and manifested itself in the form of data protection laws. Against the background of this success, the property metaphor has hardened into "owning data about oneself." Indeed, data protection laws are highly effective tools for protecting the rights of powerless individuals who, in disclosing data to a mega data controller, do not have the acumen to bargain or enforce the conditions of such disclosure.

Ownership as a Correction to Market Failure

Data ownership was an attempt to address a market failure: the data subjects' lack of bargaining power in data transactions. This is consistent with the genealogy of other forms of ownership. The idea of private land ownership originated from people's experience with the tragedy of the commons.[3] Institutions such as intellectual properties were created along the same lines, i.e., in order to encourage arts and other cultural productions which otherwise will be subject to rampant piracy and free-riding on others' creations.

In order to call something a "market failure", there has to be axiomatic values through which things are evaluated. In the case of the tragedy of the commons, the value was the production of livestock, and in the case of copyrights and patents, the values were the advances in the sciences and arts. In both cases, the values are unassailable as they are. What is data ownership trying to protect—efficiency, or more data usage perhaps? It is privacy of powerless individuals.

The fact that the forms of ownership have axiomatic values to serve means that data ownership should also be limited to the extent that it serves those values. Since the concept of data ownership was concocted to compensate for the data subjects' lack of bargaining power on the point of disclosure, and thereby prevent unwanted subsequent use and disclosure of the data about them, it is important that it is not mechanistically applied to all data but only to that which has not been made available publicly. Publicly available data has no point of disclosure that the concept of data ownership needs to intervene to strengthen the data subjects' bargaining power. The paradigmatic situation for that concept works in

the following manner: when a data subject has kept certain personal data within a zone of privacy and later transfers out of such a zone to the governments and companies, the concept of data ownership kicks in to ensure that its subsequent use or disclosure does not depart from the data subject's original will, with strong force that contractual law will not provide.

This means that the concept should not be applied to personal data that has already been published to the public on a voluntary basis without any condition. That "K.S. Park is a professor" will be exactly an example of such data. In the same vein, the data lawfully compelled into disclosure (for instance, the publicly noticed data of a company owned by a data subject) will be included. Such definition is consistent with a common sense that it is no surveillance to acquire data that everyone knows.

Indeed, a closer look at the world's data protection laws reveals a thread of such philosophy in Australia[4] , Canada[5] , Singapore[6] , India[7] , and Belgium[8] which explicitly leave publicly available data out of the purview of data protection laws. The 2004 APEC Privacy Framework also states that a data subject's right can be limited with respect to publicly available data. In 2000, the EU and the US entered into a safe harbor treaty[9] on application of the 1994 EU Data Protection Directive on U.S. data processors, which also left out publicly available data. Further upstream, the provision in the 1980 OECD Guidelines excludes from application the data that has no risk of infringing on privacy.[10]

What is more important, if data subjects can control even publicly available data about us, then the data protection laws aimed at preventing surveillance will instead do the exact opposite: We would be censoring our colleagues, monitoring them in order to watch what data they acquire, and be able to intervene when we want. Such mutual interference will empower only the powerful who can purchase censorship tools. Data protection law was supposed to be an equaliser but if applied beyond its mandate, can do the opposite in that sense as well.

To recap, what is more important is that data ownership should have their values straight to be justified as a correction to market failure. Data protection law and its incidental metaphor to ownership exist to protect privacy; in the same manner that copyright laws serve to advance the arts, patent laws, to advance science, and real property laws to maximise land use. These are all ownership or semi-ownership laws but they are all clear on what they try to achieve. What of data ownership? If it is privacy, its application should be limited to non-publicly-available data, otherwise it can erode from its socially equalising function of empowering the powerless.

Inherent Limits of Ownership

Ownership itself has a limitation as a metaphor. What does it mean to "own" something? Exclusive possession and control do not suffice because those can be obtained by virtue of contracts. Hegelian scholars got together in the 1980s in the United States to figure this out. Ironically—and somewhat tautologically—they concluded that when the statement, "someone owns something" is made, what is meant is that he/she can disown it, meaning that he/she has the legal right to transfer ownership to another person however restricted it may be. Both real properties and intellectual properties satisfy this requirement. If a person is an author of a book, and therefore the owner of the intellectual properties of that

book, that person's ownership means that they can transfer whatever Hohfeldian matrix of rights and privileges they have to another person, such that the other person has the same rights and privileges even to the exclusion of the transferor. This is a legal feat that no other person can achieve other than the so-called owner of the book.

Then, is data ownership—whether data is owned by the data subject or someone else --- a good idea at all? This article is not trying to posit that data is not conducive to ownership due to its non-exclusive and non-rivalrous nature. Data can be owned just as copyright can be owned, although the factual possibility of such ownership will be different.

However, who will own that data? Data is produced communally. Data is the result of perception. Earth itself is not data. Its presence becomes data only after there is that interaction between nature and sentient beings. It is difficult to have anyone—data controllers, data collectors, or database makers—claim exclusive dominion over such relational existence. For instance, this author is a professor only because there are "students" willing to listen to his lectures. Personal data that "K.S. Park is a professor" is the result of other people's recognition of him as a professor. His identity will be meaningful only to the extent that other individuals, i.e., students, are aware of that identity. If the concept of data ownership aims to protect privacy, that privacy is limited by the constraint that some personal data are born communal, and therefore are not conducive to ownership by any one person.

This critique is most effective against data subject's ownership—basically data protection laws—which tries to go beyond its original goal of serving privacy, and intervenes in governance of publicly available data. This concept of data ownership by data subjects may be feasible for some parts of human civilisation but not for the rest. After all, human civilisation thrives on the transfer of personal data; human civilisation is, in essence, data transfer itself. Education, literature, and arts are reflections of what we perceive and acknowledge about ourselves. Giving ourselves consent powers over these perceptions and acknowledgements can have terrible consequences on human civilisation.

Data Socialism

We should think about data socialism: the idea that data is shared amongst people as much as possible for the maximum benefit of society. This is not necessarily an opposition to data protection laws which grant data subjects ownership over data about them, thereby on the surface hampering the community use of personal data, but can be an improvement upon data protection laws by carving out a family of personal data that can be freely used for social discourse, for instance, "publicly available data" such as Singapore, India, Canada and Australia do. Also, the principles of open data and open government can demand the carving out of some personal data from the strictures of data protection law, such as court decisions database and other records of government agencies taking or deliberating adverse actions against their own citizens.

These improvements on the existing data protection laws can enhance equitable availability of AI-training data: Currently, government agencies and companies justify building the closed silos of personal data and not sharing them with people, citing the concerns of data protection laws. Some of these concerns are justified

as they are but other concerns need be moderated with or balanced against the people's need for that data for participatory democracy. Case-by-case exceptions, already built into data protection laws, are not sufficient because they will maintain chilling effects on people wishing to use the data for AI and other socially beneficial uses. Categorical exceptions need be carved out so that within these exceptions people can enjoy freedom of expression, open data, and democracy without worrying about their discourse satisfies any collectivistic (or majoritarian) notions of public interest, which often can crush beneath its pluralistic visions of a society.

In the film, Deus ex Machina, the guru reveals towards the end where he got his AI training data from: the internet. What is on the internet will be determined by data governance rules including data protection laws and the exceptions to them, as one could see what the "right to be forgotten" does to the availability of data. To allow people around the world to benefit from this learning software called AI, there should be data governance rules to allow as open access as possible to as much data as possible. Personal data normally may be deemed individually owned, but there are circumstances requiring social and communal ownership of personal data by all members of that society.

In this line of thought, Asian countries may fare better than the EU or the US because they have worked towards instituting data protection laws that are comprehensive, and at the same time have exceptions to publicly available data, thereby allowing the balance necessary for data socialism. Even still, many countries across the globe have not yet implemented data protection laws at all, or are only recently adopting them. These countries can benefit from what data-progressive countries have realised in hindsight, and create data protection laws that adhere to global standards while simultaneously being customised to that particular country's own requirements. In this manner, data protection laws will benefit data transference between and within countries, after having clearly demarcated norms that identify ownership, assure privacy, and secure against surveillance.

05 The Encryption Paradox: Examining Bottlenecks in Devising Policy Responses

Anushka Kaushik

Introduction

According to recent estimates, 22 percent of global communication traffic will be protected via end-to-end encryption by 2019. A significant number of popular messaging applications today boast of securing communication on their platforms in this manner, making the information exchanged both inaccessible and unreadable to a third party.[1] 'End-to-end encryption' refers to the encryption of messages that are in transit from a sender to a receiver, and while it is not as integrated or widely available as endpoint encryption,[2] businesses are developing more user-friendly ways to integrate it into their platforms.[3] This has easily become one of the defining technological trends in today's internet landscape.

In August 2018, the governments of the United States, United Kingdom, Canada, Australia, and New Zealand issued a joint statement on principles of access and encryption. The statement reflected on the increasing use and sophistication of certain encryption designs that present challenges for nations in combating serious crimes and threats to national and global security. While recognising that encryption is vital to the digital economy and a secure cyberspace, the statement emphasised pursuing technological or legislative methods when governments face impediments to lawful access to information for the protection of their citizens.[4] Increasingly, policymakers and legislators around the world are responding to the trend of widespread deployment of encryption in devices in order to take down obstacles to accessing private information. Yet, the joint statement, as well as the broader narrative on encryption around the world is precipitated not only by the increased availability of encryption tools. For example, the recent spate of terror attacks in various European cities has largely influenced the debate in countries like France where an amendment that could require electronic manufacturers to build back doors into their products was debated but ultimately rejected by the National Assembly. With the intention of empowering law enforcement to stem terrorist activities, other member-states of the European Union like Hungary and Poland are issuing new regulations and amendments that increase not only government access to digital data but also the scope of surveillance. In the US, Edward Snowden's revelations about mass surveillance by the government had a profound effect on the availability of strong encryption tools; perhaps owing to

the need to distinguish governmental activity from commercial products, device manufacturers have deployed default encryption systems that automatically store data in an encrypted manner.[5] In August, Facebook-owned WhatsApp rejected a demand by the Government of India to find a solution which could trace the origin of a message on its platform.[6] The company argued that traceability would undermine end-to-end encryption and affect the application's privacy protection duties.

The fact that governments want access to private information for achieving broader national security objectives is not new. However, necessitating assistance from manufacturers of encryption products, and the resulting fundamental discord between government objectives and commercial interests, make the policy process more intractable. This article analyses the bottlenecks to policy formulation that significantly slow down policy formulation, in an effort to pave the way for a better understanding of the approach that governments should adopt in mitigating technology-driven insecurity.

What constitutes a 'good' encryption policy?

Encryption policy entails the full array of government activities that guide the development, use, and adoption of encryption technology. It also speaks of a normative judgement on the part of the government about the value of such technology and is underpinned by geopolitical, social, and economic contexts.[7] Therefore, encryption policies can be directly or indirectly used to further certain objectives as they tend to have an impact both domestically and internationally. A country's encryption policy can also have ripple effects: given the massive number of interdependencies between international trade, technological trends, and geopolitics, a decision on encryption at the domestic level can impact another country's public policy, private sector, and regulatory framework. Encryption policy can be implemented via various tools which are not restricted to only legislation and regulation but also include multilateral treaties, standard-setting through cooperation with all stakeholders, exercising hegemonic status and soft power to influence other governments or corporations to follow similar regulation, and compelling private manufacturers to assist in criminal investigation, respectively.

There are numerous examples of states using one or more of such policy instruments to tackle the increasingly grey areas emerging from the widespread use and deployment of encryption tools. The Australian government released a draft of the Assistance and Access Bill in August 2018, which provides security agencies with a new set of powers to respond to the challenges posed by encryption. The explanatory document emphasises that 95 percent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications and therefore, the use of encryption is eroding the ability of law enforcement to access intelligible data. The bill broadens the obligations of domestic and foreign communication providers—which include device manufacturers, application and software providers, and carriage service providers—to allow access to communication. Moreover, it introduces new computer access warrants for law enforcement, enabling them to covertly obtain evidence directly from a device, and strengthens the ability of security authorities to overtly access data through the existing search and seizure warrants.[8] The Department of Home Affairs maintains that provisions will only be implemented within caveats like technical feasibility and

that providers will not be prevented from fixing existing systemic vulnerabilities. However, there are aspects of the bill that raise significant concerns about transparency, oversight, and accountability structures and processes.[9] It allows for a relevant government authority to issue a "technical capability notice" that would require a communications provider to build a new capability enabling police access to a device or service. This, coupled with the massive non-compliance fines makes the Australian bill one of the tougher draft legislations to be discussed by a democratic state, stoking worries of a dangerous precedent for other nations.

In the US in August, law enforcement agencies took Facebook to court to obtain access to a suspect's voice conversations on their Messenger app; the police were investigating members of the MS-13 gang.[10] Given that Messenger voice calls are encrypted end-to-end, the only way to comply with the government's demand would be to rewrite the code relied upon by all its users to remove encryption, or else, hack the government's target. Similarly, global messaging application WhatsApp, owned by Facebook, has not wavered in its stance against providing traceability to messages, arguing that doing so would rescind one of its key features, i.e., end-to-end encryption, which means the application retains no user data and access to conversations. The Indian government had demanded, among others, traceability of messages following a series of lynchings purportedly caused by the spread of fake news and misinformation through WhatsApp. These incidents are illustrative for two reasons: they indicate the different tools at a government's disposal to shape encryption policy directly or indirectly; and they highlight the perpetual disagreement between, on one hand, software companies wanting the highest levels of privacy, and on the other, state forces mandated to promote security.

What, then, constitutes a good or bad encryption policy? Is there a degree of normativity that can be attached to domestic or international policies on encryption?

At the heart of the policy debate on encryption lays the recurring privacy-security narrative that posits a trade-off between the privacy of citizens and the degree to which the state monitors and intercepts communication for keeping them secure. To a large extent, the diffusion of encryption technology to average users has been largely problematised within this dichotomy and informed by the underlying paradox: less privacy to the individual, better security for the nation. However, in the context of encrypted communications, this poses a problem as there simply is not enough data to indicate the extent to which criminal or terrorist investigations have been hampered by encryption tools. Media reports on the November 2015 Paris terror attacks, for example, quote government officials as saying that the suspects had used encrypted messaging applications to communicate with each other.[11] In the US, the Federal Bureau of Investigation (FBI) has taken Apple to court to gain access to the smartphone of one of the suspects in the December 2015 mass shooting in San Bernardino.[12] While the ubiquitous nature of encryption will be an impediment to successful law enforcement processes and its use could greatly increase in the future, there is currently a lack of empirical data that shows the magnitude of its impact. Caution must be exercised, therefore, when attributing the role of encrypted technologies in foiling overall national security objectives; any policy framework must reflect such consideration.

Encryption workarounds in the context of policy development

In the context of criminal investigations and the larger question of the impact of encrypted communications, there is another dimension that merits consideration: the existence of encryption workarounds. Defined by Kerr & Schneier as any lawful government effort to reveal unencrypted plaintext of a target's data that has been concealed by encryption, the use of encryption workarounds raises significant legal and practical hurdles.[13] The most important takeaway, however, is that the existence of workarounds could mean that encryption does not cause as remarkable a shift in law enforcement's investigative powers as thought of. Whenever targets use encryption, governments turn to a set of tools and methods to remove the barrier that denies access to private information. Kerr & Schneier identify six of them—the first three are key-based methods that rely on finding, guessing, or compelling the key which then allows decryption; the latter three focus on government efforts to exploit a flaw in the encryption system, accessing plaintext when the target's device is in use, and locating a copy of the plaintext. Each of these methods brings forth certain tradeoffs and raises questions that need to be addressed by future legal and policy frameworks on encryption. For example, accessing plaintext when the target's device is in use by gaining remote access through technical means, brings with it legal ambiguities on government hacking. There are also substantial privacy and human rights implications associated with this method, including the risk of a paucity of oversight, accountability, and transparency.[14] Similarly, governments can exploit a flaw in the encryption scheme as was illustrated in the San Bernardino terrorist attack. After Apple refused to comply with the FBI's request to disable the auto-erase feature on the iPhone, the bureau reportedly sought third-party assistance. This brought forth the question of government stockpiling vulnerabilities and whether the government should have disclosed the vulnerability so Apple could patch it. Despite the host of ethical, legal, and technical challenges, governments have encryption workarounds at their disposal and they are used, sometimes in combination, to counter encryption barriers.

Security concerns with respect to weakening encryption, in the form of providing exceptional encryption access, for example, have been well-documented and substantiated by security researchers, and recognised—in principle at least—by most governments. 'Exceptional access' is defined as giving an individual or organisation access to readable data someone has encrypted and required that the third party be granted access to the plaintext data associated with encrypted data.[15] Building on any form of exceptional access would significantly increase system complexity and features to permit such access to law enforcement could be challenging given that their use would be surreptitious.[16] Therefore, creating an exceptional access system with encryption accessible to government authorities and law enforcement officials but not to malicious actors, would be technically impossible or complex enough to implement that the overall safety of communications would suffer.[17] Such an exceptional access system would also compel companies to possibly relinquish best practices developed to make the internet and interactions through it more secure. With forward secrecy, for example, a new session key is generated for each session that a user initiates which greatly reduces the exposure of an entity that has been compromised. Since the session keys are discarded after each session, any attacker breaching a

network can only gain access to decrypted data from the breach until the breach is discovered, rendering historic data safe.[18] Therefore, mandating weaknesses in encrypted systems would not only increase vulnerabilities but also hinder innovation and development of security markets.

Challenges to formulating encryption policies

Given the myriad of technical, legal, practical, and ethical questions regarding the use of encrypted technologies and exceptional access to data, there are a number of obstacles that affect policy development at the domestic, regional, and international level. Owing to the global nature of the internet and involvement of actors across countries in availability and development of interconnected communication platforms, the effects of these bottlenecks cannot be clearly delineated at each level given considerable overlaps.

The first set of challenges arises over the question of jurisdiction. Attempting to develop any international access framework and requiring communication providers to guarantee access to numerous government agencies in countries that do not necessarily have the same legal framework would be extremely complex. Having one set of internationally defined conditions under which lawful access to encrypted communications can be granted would be an immensely arduous undertaking, not least due to the differing approaches of nation-states on freedom of communications, access to the internet, and regulation of cyberspace. There are unanswered questions regarding enforcement and compliance, illustrated in the ongoing discussions between WhatsApp and the Indian government—is it feasible for a government to mandate a feature like traceability across all applications that are used within its jurisdiction? Not only would it be difficult to get companies to comply with such a rule but mandating it would simply spur an increased use in applications like Tor or an increased use of VPNs, providing alternate methods of secure communication. Any aggressive enforcement would also negatively affect innovation and industry. The Australian Assistance and Access bill is an example of domestic policies having competing regulations to regional ones as certain parts of the bill can compel companies to override the General Data Protection Regulation (GDPR) terms in Europe and hand data over to Australian law enforcement.[19] Cross-border regulatory differences, therefore, pose an intractable barrier to developing a universally enforceable and accepted encryption policy.

The fundamental discord between incentives of the private sector—including service providers, vendors, manufactures, and software developers—to enhance the security of communications and the larger national security objectives of the government will continue to be a point of contention. A host of new developments discussed earlier in this paper, represent a technological trend aimed at providing the highest level of privacy and security of communications to the average user. Encryption technology aims to create barriers to third-party access, a property that is in the interests of law enforcement to counter during criminal investigations. The San Bernardino case is a prime example of this and there continue to be more such instances. Therefore, the extent to which third-party assistance can be mandated and necessitated by governments will be crucial. The question of jurisdiction is relevant here as well—can foreign companies be required to fundamentally alter essential features of their application, like default end-to-end encryption for example, depending on where they operate?

The third set of obstacles to encryption policy formulation raises ethical and normative considerations. While this paper has established that moving beyond the privacy-security dichotomy is crucial to developing a comprehensive approach to policy development in this area, encryption policy reflects a normative judgement on the part of the government about the value of such technology. There is a continual strain of thinking on the part of governments to gain access to encrypted communication without breaking encryption or introducing systemic vulnerabilities. Respecting trust, cooperation, and innovation in the internet ecosystem and to all stakeholders forms the benchmark of democratic digital policies. While states have recognised the significance of encryption in ensuring safe and secure communication, the implications of legislation, if it seeks to counter such provisions, on democratic values, would need to be carefully considered.

Conclusion

As businesses develop user-friendly ways to integrate end-to-end encryption, and adopt operational systems that change default local encryption setting from 'off' to 'on', aiming for the highest level of privacy and security for the user, governments face increasing barriers of lawfully accessing citizens' private information. The recent spate of terrorist attacks in Europe have largely influenced policy discussions, stoking fears that encrypted communications will significantly restrict governments' abilities to successfully stem terrorist and criminal activities. The misuse of messaging platforms by rapidly spreading misinformation has started to fuel similar conversations in India.

However, lack of sufficient data on the impact of encryption on criminal investigations and the existence of encryption workarounds at the disposal of the government may point to a less dramatic shift in governments' investigative powers than currently perceived. This also necessitates a move beyond the privacy-versus-security dichotomy that the policy debate on encryption lays within. Security concerns and the detrimental impact on innovation and industry of weakening encryption or enabling exceptional encryption access have been well-documented. These technical, legal, and practical considerations highlight the considerable hindrances to policy development in the field of encryption. There are unresolved issues with respect to jurisdiction and legitimacy of an internationally-enforceable encryption policy framework. The fundamental discord between incentives of the private sector, including service providers, vendors, manufactures, and software developers, to enhance the security of communications and the larger national security objectives of the government will continue to be a point of contention. Encryption policy debates also bring forth ethical concerns and the significance of a normative judgement that a state attaches to the value of such technology, particularly in protecting democratic principles.

The dialogue on encryption, therefore, is part of a much larger debate on security, accountability, and responsibility of internet tools. Developing an encryption policy that recognises the principles of mutual trust and responsibility between all stakeholders and accounts for the commercial interests of private companies, state security objectives, and safe online communications for the individual user will define efforts at the national, regional, and international level.

06 Cross-border Data Flows, Privacy, and India

Laura Sallstrom, Christopher Martin and Logan Finucan

Introduction

Digital data flows are the new trade in goods. 'Practically nonexistent just 15 years ago – [they] now exert a larger impact on GDP growth than centuries-old trade in goods" according to a McKinsey Global Institute report.[1] As well as driving growth, the growth of data has also driven regulation. While India's business process outsourcing (BPO) industry may be one of the world's biggest, and the country significantly benefits from global data flows, it is Europe that is driving global regulation.

As of 25 May 2018, the EU's Global Data Protection Regulation (GDPR)[2] came into effect. With implementation of GDPR, it appears that Europe has maintained its first-mover advantage, set new terms of the global privacy debate, and ignited a flurry of national privacy initiatives – Argentina, Brazil, India, Nigeria –to name a few. Importantly, in June 2018, the US state of California increased the stakes by delivering the most aggressive and most stringent piece of privacy legislation in the world: the California Consumer Privacy Act of 2018.[3] Now India is entering the privacy debate.

In an effort to get it right, the Narendra Modi government has proposed a far-reaching, GDPR-like piece of privacy legislation. A Committee of Experts under the chairmanship of retired Justice B.N. Srikrishna released the draft Personal Data Protection Bill in late July 2018 for the review of the Ministry of Electronics and Information Technology.[4] The reform is important, not only for the modernisation of India's privacy laws and the protection of its citizens' rights, but also to ensure cross-border data flows for India.

With the GDPR's requirement that a country's privacy regulations be deemed "adequate" to transfer EU citizen data (Article 45), India must reform its laws to continue to do business there. India's proposed privacy legislation is modeled on the EU's approach across many elements. It is less clear whether India's law will comport with California standards – a geographic area where many of India's crown jewel tech industries need to transfer data. In addition, aspects of the Indian draft legislation badly miss the opportunity to establish the country as a global privacy leader by embracing a nationalistic concept, one adopted by few, likely to

antagonise key trading partners, and banned by the EU — data localisation. With the draft currently under review by the government, determining the best path forward for privacy in India requires understanding both the opportunities and the risks that the draft privacy bill presents.

GDPR-lite or something really heavy

India is on the 'GDPR-lite' track: the draft privacy bill mimics the structure of the GDPR in several areas but doesn't go so far as to base the bill on the concept of a fundamental right to data privacy and loosens several standards. Like the GDPR, India's bill includes:

- Tripartite division of data subjects (or data 'principals'), data controllers (or 'fiduciaries') and data processors, with comparable obligations.

- Stronger notice and consent requirements for the processing of personal data, purpose limitation, and 'explicit consent' for the processing of sensitive personal data.

- International jurisdiction, though defined in terms of legal incorporation, not an individual's fundamental rights.

- Cross-border transfer of personal data through a combination of user consent and either a country adequacy decision, Standard Contractual Clause, or Intra-Group Scheme akin to EU binding corporate rules (BCRs).

Despite being based on the GDPR, the bill pairs looser requirements with some homegrown measures. Indian policy-makers understand the costs the GDPR would impose on the Indian economy, and therefore exempt small firms from the law and reserve particularly onerous measures (such as impact assessments, record keeping, auditing, and appointment of a DPO) for a special category of "significant" data fiduciaries.

India's draft privacy bill requires local storage of all personal data and completely bars cross-border processing of specially notified 'critical personal data'. Another category, 'sensitive personal data,' has heightened notice, consent, and compliance requirements. These provisions indicate a good understanding of the BPO industry, but are a big miss in protecting other cross-border data flows industries to and from India. Financial transactions, online shopping, and likely big data or AI projects working cross-border would all be impacted by the regulation. The business process outsourcing (BPO) industry received a generous carve out – likely in recognition of the significant and negative effect data localisation would have on that industry – but, the draft legislation fails to account for impacts on other segments of Indian industry and the overall economy. The specification that carve-outs only apply to processing of foreign data is faulty logic that is carried through the draft.

It is worth noting that the localisation approach is so potentially damaging to an economy that even the EU decided against such an approach in the GDPR. Article 1(3)[5] of the GDPR says that you cannot use protection of personal data as a reason to restrict the free movement of personal data within the EU.[6] And, the regulation on the free flow of non-personal data provides an explicit prohibition for data

localization.[7] Further EU commentary on the issue notes that the costs to the economy outweighed the benefits: 'Unjustified restrictions on the free movement of data are likely to constrain the development of the EU data economy.'[8] It is noteworthy that no such localisation provision exists in the California law, either.

What is at stake in India?

As a democratic government that respects free speech and due process, India should long have instituted a modernised and comprehensive privacy regime. With privacy regulation trending in the direction that it is, privacy laws themselves are becoming a necessity to conduct digital trade. They must be crafted correctly, however, or they will undermine the people and businesses they were meant to help.

The importance of cross-border data flows

The importance of understanding the actual size of data transactions and trade cannot be overstated, but it is also frustratingly difficult to calculate. While there are few concise data points putting a number to data flows in to and out of the Indian economy, there is ample statistical data showing that cross-border data flows are crucial to the Indian economy — and especially for the high-growth, high-skill sectors the Modi government is keen to encourage.

For example, despite the government's focus on fostering economic growth by keeping data in the country, a McKinsey Global Institute study found that the cross-border bandwidth use has grown 45 times larger since 2005.[9] This growth has had a clear boost on the Indian economy, with the Indian Council for Research on International Economic Relations (ICRIER) finding that a 10-percent increase in total Internet traffic and mobile Internet traffic increased India's GDP by 3.3 percent and 1.3 percent, respectively.[10]

Impact on sectors

The effects are also clear on individual sectors of the Indian economy. According to analysis in an IAPP article and citing the India Brand Equity Foundation, online retail in India is 'expected to grow more than 1200 percent to USD 200 billion by 2026.' The article goes on to note that at least US$9.1 billion in 2016, a figure expected to increase over 85 percent year-on-year in 2017, is driven by cross-border data flows.[11] What happens to these transactions under the proposed privacy law and data localisation provision? How can the transaction be processed?

Indian companies, from start-ups and SMEs to conglomerates and multinationals, are increasingly reliant on cross-border data flows owing to their digitalised production chains — including outsourcing, manufacturing, fintech, e-commerce, and healthcare. The free flow of data promotes investments in innovative technologies and the cloud ecosystem, improves supply chains, and helps lower the barriers to accessing financial and medical services, among others. For example, some of India's most innovative companies, such as Myntra, Flipkart, and Fortis Healthcare, rely on global cloud services and data centres outside of India to deliver their services at the lowest cost possible and still remain competitive. The recommendation to localise personal information will likely impact the services of these and similar companies.

Underpinning many of these sectors are digital payments, which are growing at 30 percent annually.[12] Further growth here is a priority of the Modi government. Since many of the payment facilitators are providing global services, cross-border data flows are necessary. After all, it is impossible to conduct an international transaction without some data moving across a border – so this also impacts India's data exports. For further consideration, according to the Brookings Institute, over 40 percent of India's goods and services exports consist of software services and IT-enabled services (ITES) from financial analysis, accounting, medical transcription to the provision of applications for smartphones.[13] The impact on these industries would be dramatic.

The future of growth

Cross-border data flows are therefore essential for preserving India's gains in these areas, and disrupting them risks disrupting the jobs, growth, and innovation that these sectors contribute. It also risks India's future; the Brookings Institute found that had India accelerated its participation in all types of global flows – including data flows – to match the performance of leading countries between 2004 and 2014, its GDP would have been US$1.2 trillion – or 58 percent – higher.[14]

Research has shown that data localisation could reduce domestic investments considerably. In modeling the impact a data localisation provision would have in various markets, the research projected substantial reduction in domestic investments as follows: in China by 1.8 percent; in India by 1.4 percent; in Indonesia by 2.3 percent; in Korea by 0.5 percent; and in Vietnam by 3.1[15] percent. Exports could also fall by up to 1.7 percent in some countries due a direct loss of competitiveness.[16]

According to a study by Leviathan Security, such measures will also raise the cost of hosting data by 30–60 percent, thus increasing the financial burdens for small and medium companies and start-ups.[17] Therefore, efforts in the draft legislation to protect the small and medium sector from the burdens of the legislation will be mooted by the data localisation requirement's overall impact on the economy and the tech sector that services smaller companies.

Reciprocity

From a policy planning standpoint, policymakers should think of adequacy as a modified version of reciprocity. In privacy language, and driven by the EU, it is a statement that trading partners must meet the EU's standards of privacy in order to trade with the EU. Agreements like Privacy Shield provide mechanisms to meet these standards. Nonetheless, this is fundamentally a bilateral negotiation.

For further consideration by policy-makers, standards for trade in data are evolving on this subject. At the moment, trade protection for data is limited to a few bilateral and multilateral trade agreements or the unclear protection of the WTO services agreement. In short, trade in data is largely subject to the bilateral whims of trading partners. With this in mind, the government may want to consider the following as it makes plans to secure India's future for leveraging and trading in data:

First, nearly a quarter of India's IT-enabled exports went to the EU in 2016-17.[18] Despite being influenced heavily by the GDPR, it remains unclear whether the EU will grant India an adequacy determination under the proposed framework. The EU has been primarily focused on the impact of US tech companies on European data, but that is likely to change as this draft draws attention to India's growing role in global data processing.

Second, California's own privacy law has not influenced India's draft, having been published only recently. Nevertheless, compatibility with it could be just as important given the concentration of global tech companies in the state. India's data localisation and more flexible privacy provisions in some areas could bring the two laws into conflict, threatening data transfer – and therefore the ability to operate in India – for many prominent companies.

Finally, and perhaps worse, California's law brings pressure on the US government for a federal law. With an activist and anti-trade US administration that uses reciprocity as a trade tool, the conflict of concepts - particularly the data localisation provision—could become a privacy or a trade issue. It would not be difficult to imagine, for instance, the Trump trade team deploying a reciprocal ban on transfer of US data to India.

Conclusion

India's economy depends on cross-border data flows and has much to gain by embracing the benefits of data. In order to continue to trade with key partners, India must enact privacy reform. However, it is unclear if the current bill will meet a GDPR standard, or the more stringent California standard. Further, the government has proposed the concept of data localisation which has the potential to limit India's economic growth and fails to contemplate the impact of those provisions on all segments of India's economy. Given the size of the technology sector and India's role as a beneficiary of data flows, the country should be a global advocate for moderate privacy regimes, free transfers of data, and opposing data localisation proposals in other markets. A forward-looking privacy and data strategy will be less concerned with keeping data in the country and more concerned with ensuring Indian access to data of other countries' citizens.

(The authors thank Ryan Johnson, Filip Pacyna, and Halak Mehta for their research assistance.)

07 Digitalising India's Cultural and Creative Industries Byte by Byte

Lina Sonne

Introduction

India's cultural and creative industries have for a long time been dominated by films and TV, and today this is mirrored in the emergence of digital content primarily taking the form of video. Yet, beyond the moving image, India's arts and culture traditions are rich and diverse, straddling both the traditional and contemporary forms of Indian and Western arts and culture. These cover a wide range of fields, too—including visual arts, performing arts (theatre, dance and music), literature, crafts, and fashion. Live performances and festivals have become popular in the last few years, such as biennales and literature festivals to various classical and modern music festivals. New forms of expression are emerging, whether spoken poetry, street art as a form of public art and beautification, or the multilingual rap and hip-hop scene.

That India's cultural and creative industries are changing is evident from the cultural landscapes in India's main metropolitan cities that are becoming more vibrant in cultural activity, the number of new venues opening up across different parts of the country, as well as the growth of new partnerships and the emergence of news ventures and business models. The sector grew by 13 percent during 2017, and was worth an estimated INR 1.5 trillion.[1] The growth of segments that utilise digital technologies including animation, gaming and music, as well as video content creation, and business models that benefit from digital advertising and brand building are especially impressive.

This article offers a broad overview of how digitalisation is currently impacting India's cultural and creative industries.[2] It uses the term "cultural and creative Industries" (CCI), and considers it to broadly encompass visual and performing arts; films; video and broadcasting; new media; media and publishing; gaming; animation, visual effects and post-production.[3]

Facets of Digital Cultural and Creative Industries

A number of disruptions are taking place as the production and consumption of arts and culture is going increasingly digital. The following sections will discuss in turn six facets of digital cultural and creative industries.

1. Consumption: The Ubiquitousness of Video Content on the Mobile Screen

The introduction of cheaper smartphones, together with low-cost data plans (such as that of Reliance Jio) has led to a rapid rise in mobile phone ownership in India. The number of mobile subscriptions was pegged at 1,183 million as of March 2018.[4] In turn, access to mobile phones has expanded the reach of the internet; there were 456 million users in India by December 2017.[5]

Today, as much as 77 percent of online media consumption in India is done from a mobile device.[6] For Indian language users, that number increases to 99 percent.[7] At the same time, 95 percent of Indian households own only one TV[8] and few have access to a video recording device. The mobile phone therefore reigns supreme in both offering an additional screen, while also enabling flexible viewing. Many consumers view digital content while on the go – commuting, travelling, or simply seeking privacy while outside the home, rather than in the home or office.[9] This has caused the death of primetime TV as the world knew it.

In 2017, a year of rapid expansion of mobile phones with data plans in India, online video consumption grew by five times, and over 90 percent of the time spent watching was on mobile screens.[10] Given that videos are primarily watched on mobile phones, consumers prefer short-form, or "snackable" content of up to 20 minutes—this has shifted the focus of producers and content creators towards short content.[11]

However, even as the reach of mobile phones with cheap data plans has expanded rapidly, poor bandwidth is still a concern in India. Therefore, content producers must enable consumers to watch online content offline to scale across the country—something that has been introduced by YouTube, for example.

2. Democratisation of Content Production and Distribution

Digital and technological advancement have ensured that the production and dissemination of content has become cheap enough while maintaining adequately high quality. Scale has therefore ceased being a requirement for production; large studios, production houses and media corporations no longer dominate the production of content, and the sector is being democratised. This is why today, content can be created by a wider range of producers: large companies such as Eros International and Viacom 18, small local ones building their own music studios, young entrepreneurs sourcing local stories across India, YouTubers (e.g. MostlySane and BeYouNick), and start-ups producing content online, for example Pocket Aces, All India Bakchod (AIB) and The Viral Fever (TVF). There are also the freelancers working on advanced animation and gaming worldwide, while sitting in India.

This bottom-up content production has resulted in much more diverse content, beyond the Bollywood films and soaps that dominate TV entertainment. Digital content is more personalised given the much closer connection and interactions between the content's creators and their content consumers via social media.

While grassroots content creation (such as rural community radios) has long existed within the remit of community development in India, it is now going digital. For example, Khabar Lahariya[12] is a women-run digital-first rural news reporting platform that employs a network of local reporters.

Meanwhile, Over The Top (OTT) platforms such as Netflix, Hotstar, Amazon Prime and Reliance Entertainment are partnering with production houses to sign on films to stream as well as new serials (E&Y, 2018), as well as with content start-ups such as AIB, and film producers for serials (e.g. Netflix productions Ghoul and Sacred Games). These OTT platforms have in turn driven up demand for new content as well as changing consumer demand for content in India.

Platforms such as YouTube and Facebook have broken down distribution and entry barriers by offering platforms on which any creator can distribute content. Many content start-ups in India, therefore, started out producing content via YouTube and Facebook (e.g. AIB, Pocket Aces and Bharatiya Digital Party). The music industry has seen the most staggering change in terms of content distribution, with 70 percent of total music revenue in India coming from digital music.[13]

Apart from professionally generated content, user-generated content has been exploding on the Indian scene in the last couple of years. For example, livestream app 'Bigo Live' had more than 40 million downloads in India alone by the end of 2017.[14] Such livestreaming platforms have become popular across the country, and especially outside of the main metros. Interestingly, Bigo Live does not rely on advertisement, but on user subscription and in-app monetisation.

3. Regional Language Content: the Next Frontier

Regional language content in India is experiencing an online renaissance. In 2017 there was a 100-percent growth in watch time on YouTube for regional content, for example,[15] and 95 percent of all video consumption in India is now in regional languages.[16] This in spite of the fact that content in Indian regional languages is only one percent of available content in English.[17]

The trend is set to continue with nine out of every 10 new internet users likely to be regional language users over the next 15 years.[18] Moreover, small cities with up to one million inhabitants had the highest growth rate in watch time in 2017,[19] and non-metros were responsible for the 71-percent growth in demand for Video on Demand,[20] suggesting that growth in non-metro viewing is also fueling expansion in regional language viewing.

Indeed, the digital revolution is resulting in the opening up of new markets for content.[21] Content in languages with limited existing content—including Oriya, Bhojpuri, Assamese and Gujarati—is growing at twice the rate of content in Hindi, Telugu and Tamil, which have more established industries that create content.[22] Clusters of regional content production are emerging, with regional language start-ups such as Bharatiya Digital Party (Marathi), Sakkath Studio, (Kannada) and The Comedy Factory (Gujarati) now engaging with content providers who are looking to expand their semi-rural and small town reach through regional language content. Likewise, platforms such as Roposo allow consumers to share, create and engage with content across multiple regional languages, and Kavi Puvi Viamedia is a platform offering entertainment in South Indian languages.

The use of regional language internet is primarily for entertainment, particularly through video. Growth is hampered to some extent by poorly developed standards for digital scripts in regional languages.[23] This makes it hard to not only provide and consume written content, but also to navigate and search online for video content, as well as in creating communities that engage with content the way English language content users do. However, there are efforts underway to improve and eventually standardise digital fonts in regional languages. One recent initiative to improve the availability of regional written content online is Navralekha by Google, which will help to publish offline regional content online.[24]

4. Experimental Business Models, a Bubble, and the Monetisation Conundrum

Digital content start-ups are multiplying and venture capital is flowing into the sector at such a rapid pace that there is talk of a "digital content bubble". It is forecasted that some US$ 400 million would have been so far invested in Indian content start-ups in 2018.[25] While this figure includes a large number of deals in the education space, there are several notable start-ups in the cultural and creative industries, including self-publishing platform Pratilipi, entertainment content platforms like Pocket Aces, and regional language content platform Roposo, which have received venture funding.

In spite of the increased interest from investors, across content production and distribution, business models remain experimental in nature, as few have found viable long-term sustainable models. There are broadly three ways to earn income: advertisement, sponsored content, and subscription fees. The OTT segment, for example, relies largely on advertisement revenue[26] while smaller content creators earn income from sponsored content, including corporate content, and the sale of content to large OTT platforms such as Netflix and Hotstar. Subscription models have so far had limited success as Indian consumers are reluctant to pay for content, with only one to two percent of them currently paying for digital media content.[27] Furthermore, ticket sizes of subscription or membership fees are small, which means companies require substantial scale to ensure a sustainable revenue stream. The next five to 10 years are therefore likely to see consolidation in digital content as venture funding dries up and the current high demand for new content flattens out.

5. Beyond Content: Online Networks, Consumer Engagement and Digital Archives

While the spotlight has fallen on online content, digital change is revolutionising many aspects of other areas of the cultural and creative industries, too.

New Platforms for Consumer and Audience Engagement

Social media has provided new channels for reaching and building audience engagement, for example through platforms such as Facebook and YouTube. Emerging artists are able to boost their reach, and build a following that sometimes converts into more conventional distribution opportunities (e.g. being signed by a record company).

Likewise, the advent of social media tools such as Instagram allows local initiatives to have a global reach. This has been the case for Delhi-based street art organisation, St+art India Foundation, which undertakes local street art projects in various cities, including Delhi, Mumbai and Hyderabad. The digital evolution has resulted in new ways of selling art, with online platforms such as Mojarto and Saffron Art able to reach a wider audience than brick and mortar galleries. Meanwhile in Mumbai and Delhi, 'Carpe Arte' has built an online network of visual arts enthusiasts through regular gallery walk-throughs, artist studio visits, and listings of events, thus combining audience engagement online with providing information on events where there are no event aggregators.

In publishing, meanwhile, traditional bookshops are facing stiff competition from online outlets that sell books (Amazon and Flipkart), online publishers like Juggernaut, a mobile-screen first publisher and platform, and self-publishing platforms such as Pratilipi. A similar story has emerged in the news media, where newspapers are competing with online-only news outlets including Scroll, The Wire, Quartz India, The Quint, as well as aggregators like Firstpost, Buzzfeed India and DailyHunt.

Nevertheless, digital monetisation remains an issue, with digital publishing contributing to only about five percent of print companies' total revenue.[28] Few online news media platforms, meanwhile, are able to charge subscription or access fees of any kind.

Online Networks and Access to Funding, Support and Markets

The cultural and creative industries have a large number of individuals and organisations that form part of the gig economy. As such, it is important to have access to new online networks listing opportunities for funding and work, as well as creating a space for peer-to-peer engagement and finding potential collaborators, such as the Arts & Culture Resources in India (ACRI) network. Furthermore, crowdfunding platform Wishberry offers an alternative to limited conventional sources of funding for arts and culture in the country.

At the same time, digitalisation has created a market for new types of intermediaries, such as multi-channel networks (MCN) like WhackedoutMedia and Culture Machine, that work with creatives in production and distribution, driving digital traffic, and monetisation.[29] The increased need for new, high-quality content both in India and internationally has also driven up demand for specialists in animation, visual effects and post-production.[30]

Museums and Galleries: Digital Archives, Access

Museums and galleries in India, such as Delhi's Kiran Nadar Museum of Art, are increasingly using social media to reach a wider audience. In Mumbai, the Bhau Daji Lad Museum can now be toured digitally as part of Google Arts and Culture (formerly called the "Google Art Project"), which brings offline collections online to a global audience, one museum at a time.[31] In Kolkata, Jadavpur University is creating a digital archive of North Indian classical music.[32]

The Government of India is creating a digital archive of its museum collections, such as that of the National Gallery of Modern Art (NGMA), and is currently undertaking

a large-scale and state-wise mapping of the country's arts and culture.[33] To date, archiving and mapping of arts and culture artefacts has been limited in India over the last few decades, and the advent of digital archiving is a turning point, and is expected to inform policy going forward.

6. Policy Vacuum and the Challenge of Piracy

India does not currently have a single, central arts and culture policy. To complicate matters, multiple ministries govern various aspects of the cultural and creative industries, from the Ministry of Culture, Ministry of Tourism, Ministry of Information and Broadcasting to Ministry of Textiles, and Ministry of Electronics and Information Technology. In other words, multiple policies and schemes from the Government of India and State Governments support the cultural and creative industries.

There is currently a policy vacuum with respect to digital arts and culture, and especially digital content production and distribution. Unlike broadcasting and films, there are few restrictions on content delivered via data. The lack of checks and balances offers greater freedom for creators, but brings with it the risk of poor or illegal content being created and distributed. Both professionally generated and consumer generated content is today essentially self-regulated, either by creators or content-sharing platforms.

One area of regulatory oversight that is a considerable challenge for the industry is that of weak intellectual property (IP) and copyright. It is estimated that India's film industry loses US$ 2.8 billion a year due to piracy.[34] Without clearer rules and better enforcement of IP and copyright regulations, there is a risk that digital business models in the cultural and creative industries will find it increasingly difficult to become sustainable.

Conclusion

India's cultural and creative industries are at an exciting inflexion point. The opportunities for the country to create a digital cultural and creative industries at par with leading global hubs such as London and New York are visible. However, to make the most of such opportunities, India also needs to ensure that there is an enabling policy and regulatory environment, that the basic infrastructure including electricity and access to internet is working, and that individuals, start-ups and established companies are able to work within a well-functioning ecosystem.

Today, even as there is a great deal of start-up activity across India, a supportive ecosystem does not exist. There are no easy ways, for example, to access finance, to seek information or to find collaborators. Different segments of the cultural and creative industries exist in different islands, and little collective work is undertaken by umbrella organisations to create a cohesive 'industry' ecosystem. Such an ecosystem would need to bring in higher education to the fold to ensure the industry is able to benefit from talent with the required skills set. Likewise, the sector needs better information on what works and what does not, which given the lack of research, is largely absent today.

08 Breaking the Linguistic Barriers to Accessing the Internet

Ashwin Rangan

More than half of the world's population are now online, yet billions of people remain disconnected from the global internet economy largely due to lack of access. The main barrier is the lack of infrastructure such as adequate devices and 3G or 4G connectivity. The other reasons why a significant population continues to be disenfranchised include lack of computer literacy, as well as the dearth in content in local languages.

Improving the linguistic diversity of an internet world that is dominated by English is an important step to bringing the rest of the world online. A majority of the next billion internet users will be from the Asia-Pacific region, and most of them do not use English as their first language, if at all. According to a study by consultancy firm KPMG, "there will be over 536 million internet users in India who will use only the Indian languages by 2021. The use of Indian languages on the internet is growing at 18 percent per year, whereas the growth of English as medium on the internet is pegged at only three percent". This trend is expected to be repeated in other parts of the world as people continue to access the internet in their native languages.

Therefore, the governments, businesses and technology industry need to work together to foster an ecosystem that enables the non-English-speaking communities to get online. Connecting the unconnected would mean increased economic activities and improved access to education, healthcare and e-government services. For businesses, this means an opportunity to tap the untapped market of nearly half the world's population.

The internet infrastructure has evolved considerably to reduce the language barrier. However, a lot more needs to be done to realise a truly global internet.

Understanding the internet infrastructure

A central part of the internet is the domain name system (DNS) which helps the users find their way. Every device on the internet has a unique address – just like a telephone number – which comprises a string of numbers called an "IP address" (for "Internet Protocol"). As the IP addresses are difficult to remember, the DNS makes it easier to use the internet by allowing a familiar string of letters (the domain name) to be used instead of the arcane IP address.

The Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation, has been entrusted with the responsibility of ensuring stable and secure operation of the internet's unique identifier systems by the global internet community. The ICANN coordinates the allocation and assignment of names in the root zone of the DNS, in addition to other functions. (The author is senior vice president engineering and chief information officer of ICANN.)

In 2012, the ICANN rolled out a new generic top-level domain (New gTLD) programme – an initiative enabling the largest ever expansion of the DNS. It is aimed at enhancing innovation, competition and consumer choice as well as supporting a secure, stable and resilient internet. Through the introduction of more than 1,200 new top-level domains (TLDs) – which are the letters found at the end of an internet address (such as .com, .net or .org) – the programme has enabled hundreds of new TLDs that are longer than the traditional two or three characters and/or are in different scripts (known as 'internationalised domain names' or IDNs)[1] to enter into the internet's root zone in recent years (IDNs were first made available for governments and administrators of countries/territories operating country code top-level domains in 2009).

This means that today's TLDs speak to interests and affiliations (e.g., .COLLEGE or .PARIS) or are in languages other than English (e.g.,世界or онлайн)—enabling non-English users to have domain names in local languages and scripts – such as Gujarati, Arabic, Chinese, Cyrillic, Devanagari and many more.

Challenges in achieving a truly global internet

Though the expansion of the DNS is critical in bringing the next billion people online, giving new users a choice in their online identity, and expanding the global internet economy, the incorporation of new domains across the global internet is not automatic. The internet infrastructure may have grown dramatically in recent years, yet the software that supports the internet-connected applications has not – it is still based on the rules set up more than two decades ago.

Therefore, even though the domain names in local scripts (IDNs) are now acceptable, there are slight differences between the scripts which could cause confusion. For example, the Chinese domains can be written using the traditional Chinese or simplified Chinese characters. Some words in the Latin script can be written in the same visual form using the Cyrillic script. Unless identified and managed, these variant labels, as they are called, can pose usability and security challenges.

In 2015, a Neo-Brahmi Generation Panel (NBGP) was set up to develop such rules for nine scripts used in South Asia – Devanagari, Gurmukhi, Gujarati, Oriya, Telugu, Kannada, Tamil, Malayalam and Bangla. The NBGP members comprise of more than 60 experts in technology and linguistics from Bangladesh, India, Nepal, Singapore and Sri Lanka. The NBGP has already finalised the proposals for many of these scripts, which are currently undergoing public review,[2] and aims to finish its work in the coming months.

Due to the rapidly changing domain name landscape, many systems do not recognise or appropriately process new domain names, primarily because the TLD may be an IDN or more than three characters in length. Not all online portals are primed for the opening of a user account with one of these new email addresses.

While filling out online forms, the TLDs that exceed the previous standard length of two or three characters and the email addresses that are based on non-English scripts are not always accepted. When this happens, it locks the users out of the organisation's offering and prevents them from experiencing the full benefits of the internet.

This challenge is remedied by a state known as 'universal acceptance' (UA), which is a technical compliance best practice that ensures all domain names and all email addresses can be used by all internet-enabled applications, devices and systems. New standards in email, known as 'email address internationalisation' (EAI), have also been introduced to accommodate email addresses based on the IDNs.

Fortunately, the UA compliance is considered a simple "bug fix" or routine update to online systems. A group of companies including Afilias, Apple, GoDaddy, Google, ICANN, Microsoft, Verisign and many others have formed a consortium called the Universal Acceptance Steering Group[3] to help raise awareness of the UA and provide guidance and resources for becoming UA-ready.

The benefits of UA are numerous. A recent study[4] estimated a potential US$9.8 billion revenue growth opportunity from both the existing users using the new domain names and from the new internet users coming online through the IDNs. This is a conservative estimate as it does not take into account the potential future growth in the e-commerce spend or in the registrations of new domains. It also looked at only five major languages and language groups that would benefit from IDNs – Russian, Chinese, Arabic, Vietnamese and Indic language groups.

From a social and cultural perspective, the report also showed that when governments and non-governmental organisations (NGOs) become UA-ready they will be able to engage better with their citizens and communities who want to choose their own identity with their own domain name, whether in English or non-English scripts.

Progress and next steps

The good news is that organisations and governments around the world are taking meaningful steps toward UA-readiness – particularly in countries like China, Thailand and India which are expected to be in the forefront of adopting the IDNs and resolving the UA challenges. The cloud-based email services of Microsoft and Google are able to both send to and receive from all valid email addresses – meaning, they are EAI-ready. An Indian company, Data Xgen, is already providing email services in the Indic scripts. Also, the Indian government has launched a Dot Bharat ( ) domain in multiple scripts – an important step in helping the non-English-speaking communities access the internet.

Indeed, these are exciting times as the internet evolves to becoming truly global. In the multi-lingual, multi-script India, the fastest growing large economy, the number of internet users grew more than 28 percent in 2016 but could bring about only 27 percent online penetration, according to the 2017 Internet Trends Report. Therefore, a significant internet growth is still to come. Around the globe, an improved access to wireless broadband, growth in smart phone usage and e-commerce innovations are leading to increased demand for internet content and

services in the markets where most residents speak non-Latin-based languages. Regardless of the language they speak, there is much to be gained through the widespread adoption of the IDNs and by updating the software systems to work in harmony with the common internet infrastructure.

09 Foundations of a Potential Executive Agreement between India and the U.S.

Justin Hemmings and Sreenidhi Srinivasan

As the Indian Parliament considers its draft Personal Data Protection Bill, a key question will be about the strategy that the Indian government selects for addressing cross-border data flow issues, particularly for matters of law enforcement. As a co-author of this article (Hemmings) has discussed previously,[1] the existing Mutual Legal Assistance Treaty (MLAT) framework has struggled under the increasing weight of requests for electronic evidence. In particular, requests to US-based service providers for electronic evidence currently face wait times of approximately 10 months as the US Department of Justice contends with an increased volume of requests and the need to help requesters meet the unfamiliar requirements of US criminal procedure.

The Personal Data Protection Bill addresses the issue of cross-border data flows for law enforcement through a new data localisation requirement. Clause 40 of the Bill requires that "[e]very data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data" covered by the act.[2] This clause also authorises the Central Government to classify certain categories of "critical personal data" that can be processed only in a server or data centre located in India.[3] By ensuring that data related to Indian data subjects is stored within the clearly defined reach of Indian law enforcement, this requirement would sidestep the need to use mutual legal assistance procedures like an MLAT request.

Data localisation can also create unintended economic consequences, however. In response to the draft Bill, Telangana's IT minister expressed concerns that this requirement would hurt Telangana's start-up businesses and discourage foreign investments in the state.[4] Other stakeholders have argued that localisation can present a trade barrier for Indian start-ups looking to expand globally.[5] Localisation requirements can also stunt technological innovation and growth that relies on the ability to transfer and replicate data in efficient ways.[6]

An alternative to data localisation that the Indian government should consider is new mechanisms for acquiring electronic evidence including the US Cloud Act. While India may not be able to meet all of the Cloud Act's eligibility requirements today, the Indian legal system provides a foundation that, in combination with modest changes and a carefully crafted executive agreement, could enable Indian

law enforcement to request evidence directly from US-based service providers. As US-based companies build new mechanisms for handling increased direct requests for data, a Cloud Act executive agreement between India and the US would allow India to take advantage of these expedited procedures without discouraging economic growth and investment.

This article examines existing procedures and principles of Indian law that could be used to craft a Cloud Act-compliant special procedure for Indian law enforcement to order US-based companies to produce electronic evidence.[7] In particular, this could be accomplished by including principles enshrined in the Indian Criminal Procedure Code ("CrPC") and the Information Technology Act 2000 ("IT Act") and its attendant rules. Building on these foundational elements, this article will show how India can create a parallel specialised procedure that would meet the Cloud Act's requirements without requiring India to pass sweeping new legislation or fundamentally alter its existing criminal procedure and practice. Part 1 outlines the Cloud Act's requirements for non-US legal processes to demand access to electronic data within the US. Part 2 examines existing procedures for obtaining electronic evidence under Indian law. Part 3 examines how existing procedures in Indian law could be implemented to create a Cloud Act-compliance process for law enforcement to demand access to electronic evidence.

The Cloud Act's Requirements for Foreign Evidentiary Process

For foreign governments seeking eligibility to enter into a Cloud Act executive agreement, 18 U.S.C. § 2523 contains a number of requirements related to the foreign government's legal system and procedures. These requirements include detailed requirements for any order issued by the foreign government subject to a Cloud Act executive agreement. Any order shall:

(i) serve the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

(ii) identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order;

(iii) comply with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

(iv) fulfil requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation; and

(v) subject itself to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order.[8]

While these particular requirements are new to the US Cloud Act, similar requirements on content and form are already present in the MLAT between India and the US. For example, where the Cloud Act limits its scope to serious crime, the India-U.S. MLAT outlines the types of offenses for which a country can refuse to provide assistance (e.g., actions considered criminal under military law

only or political offenses).[9] The Cloud Act's requirements to identify a specific object of an order likewise parallels the MLAT's requirement that a request provide a description of the evidence, information, or assistance sought, including any available information on where the information may be located and any individuals or entities in control of the data.[10] Where the Cloud Act requires that the order be based on domestic law, the MLAT also requires that a request include a description of the nature of the investigation, prosecution, or proceeding, including the specific offenses related to the matter.[11] Finally, while the MLAT does not require that a request contain "articulable and credible facts," in practice because the request must be executed under US law, including the requirements of the Fourth Amendment, a request to the US. would need to go beyond the Cloud Act's requirement and make a showing of probable cause in order to be fulfilled.[12]

Where the MLAT between India and the US enables diplomatic requests for assistance, a Cloud Act executive agreement between the US and India would allow Indian law enforcement to order US-based service providers to produce evidence solely under Indian legal authority. In other words, while Indian law enforcement may be familiar with making requests with requirements similar to those contained in the Cloud Act, in this case Indian law itself must provide a procedural avenue for requests that meet the specific requirements in the Cloud Act. And unlike an MLAT request, these procedures must also be subject to review or oversight by an independent authority.[13]

Authorised Investigatory Powers under Indian Law

Indian law enforcement has the authority to order the production of electronic evidence under a number of different authorities, including the Code of Criminal Procedure and the Information Technology Act. In practice, Indian law enforcement generally relies on its authority under Section 91 of the CrPC to require the production of any document "necessary or desirable for the purpose of an investigation, inquiry or trial" under the law enforcement officer's sole authority.[14] Unsurprisingly, it appears that law enforcement regularly makes use of this broad authority, even continuing to order the production of data under the CrPC despite stricter provisions in other specialised statutes like the IT Act.[15]

Section 91 also authorises courts to issue summonses for the production of data, as long as the document satisfies the same "necessary and desirable" standard. Case law suggests that this authority has typically been used by the accused, complainants, and prosecutors who would petition the court to compel the production of documents at various stages of a trial. The Indian Supreme Court has noted, however, that a police officer could petition the court and compel the production of evidence "for the purpose of an investigation, inquiry, or trial."[16] Under that interpretation, a law enforcement officer would be able to request a judicially authorised order for evidence, which would arguably satisfy the Section 2523's requirement that an order be independently authorised.

Section 93 of the CrPC also authorises the court to issue a search warrant if it has reason to believe that the object of the warrant will not produce the information sought pursuant to a Section 91 demand.[17] In issuing a warrant, the court may specify the place where the warrant authorises law enforcement to search for the information specified. Notably, however, these search warrants do not have any other requirements and limitations. Section 93 also explicitly permits general

warrants where the information sought is not known to be in the possession of a specific person,[18] or where the court believes the proceeding will be served by a general search or inspection.[19] While such a generalised warrant would fail the Cloud Act's specificity requirement,[20] it is not necessary that all potential versions of the procedure comply with the Cloud Act, but rather only those seeking evidence under the executive agreement.[21]

The IT Act also provides specialised procedures for computer-related crimes and electronic information, and explicitly notes that it supersedes any other inconsistent provisions or laws.[22] Notably, under the IT Act a law enforcement officer does not possess the inherent authority to compel the production of evidence–this suggests that for information under the scope of the IT Act, any attempt to rely on Section 91 of the CrPC would be unauthorised. Instead, under the IT Act the Central or State Government can direct any agency of the appropriate Government to intercept data if it is "necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, [or] security of the State" or other specified circumstances.[23] The Government can prescribe procedures and safeguards for this purpose and has issued the (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules ("IT Interception Rules") that, in part, define the term "intercept" as including the "viewing, examination or inspection of the contents of any direct or indirect information."[24] While these provisions of the IT Act and its accompanying Rules appear to address procedures for conducting real-time interception of data, the Act also specifically permits authorizing the Government to intercept "any information generated, transmitted, received or stored in any computer resource" and can compel the intermediary or person in charge of the targeted resource to "provide information stored in [the] computer resource."[25] The IT Act does not, however, provide for independent judicial authorisation or review of any such order as the sole authority lies within the specified Executive branch officials. As such, an order issued pursuant to the IT Act could not on its own meet the Cloud Act requirements as they stand, though the Act or even the rules could conceivably be amended to permit submission of an order to an independent judicial authority for review in cases where the order is intended to operate under the Cloud Act executive agreement. Even if the IT Act itself does not ultimately house the procedure that law enforcement uses under the executive agreement, these particularised procedures and safeguards for stored electronic data demonstrate an acknowledgment that these types of data warrant a particularised approach beyond the broad law enforcement authority of Section 91 of the CrPC.

Implementing a Cloud Act Executive Agreement under Existing Indian Law

Based on current structures in Indian law, one can envision a Cloud Act executive agreement that would authorise a specialised process for Indian law enforcement to make direct demands of US-based companies for electronic evidence. First, in order to ensure that the requirements are applied uniformly, an executive agreement could specify that requests must be issued by a single agency. The Indian Central Bureau of Investigation (CBI) could perhaps fit the bill for this purpose and the CBI could designate one or more units that would be expert in complying with the executive agreement's other requirements (e.g., specificity).[26]

Having a limited set of authorised points of contact would also facilitate the monitoring and auditing of procedures required under the Cloud Act,[27] where attempting to grant broad authority to all law enforcement officials would make oversight, at best, unwieldy.

CBI could also make use of the existing authority under Section 91 of the CrPC to seek issuance of summons or Section 93 of the CrPC to seek judicially authorised search warrants.[28] While this may be a novel exercise of authority under the CrPC, the existing case law suggests that it would be a permissible exercise of that authority which would also likely satisfy the safeguards required in the Cloud Act. If, however, the IT Act were to be interpreted to occupy the field for requests regarding electronic evidence, the law or at least the rules would likely need to be amended to enable processes that could meet the Cloud Act requirements. For example, executive agencies could instead submit their orders to a qualified independent magistrate for review, either before, concurrent with, or after their execution to ensure compliance with the IT Interception Rules. Such a review would need to be undertaken by a body outside the Executive branch in order to qualify as "independent" under the Cloud Act, though it is possible that a sufficiently insulated executive authority might also be sufficiently independent. The IT Act could also potentially be amended to allow CBI, or a specialised CBI sub-unit or units to exercise the authority to compel the production of stored evidence, pursuant to independent review. Housing this procedure within the IT Act would also avoid any possible pre-emption challenges, as the Act specifically supersedes other conflicting laws.[29]

Conclusion

While the Personal Data Protection Bill as written may not meet the Cloud Act's requirements for an executive agreement, existing procedures and principles of Indian law could likely be leveraged to create a specialised process that would meet the Cloud Act's safeguards. Carefully crafted search warrants issued pursuant to Section 93 of the CrPC offer one such path to a qualifying order, while the IT Act provides an expandable framework that could also conceivably be leveraged under such an agreement. In either case, pursuing these means for accessing electronic data held in the US would serve to both ease the current burden on law enforcement authorities feeling stifled by a lack of access to evidence, while avoiding the potential economic and privacy risks of a data localisation requirement

10 Securing Digidhan: A Cybersecurity Approach for India's Digital Payments Bet

Sidharth Deb

Introduction

The launch of the 'Digital India' campaign in 2015 signalled a paradigm shift for India's policymakers. The programme is a concerted attempt by the Indian government to leverage the transformative capacities of information and communication technologies (ICT) toward a "... digital(ly) empowered and knowledge society".[1] Given the catalysing potential of internet and telecommunications deployment, the Indian government has placed its collective bets on leveraging such mediums of delivery to engender access to crucial services and utilities that are essential to the attainment of socio-economic inclusion.

Under this umbrella initiative, the policy of mobile and internet-led financial inclusion has assumed a greater sense of importance. This was underscored by the Indian government's announcement in November 2016 of the demonetisation of 500 and 1,000-rupee notes—thereby invalidating over 86 percent of the country's cash circulation. Perhaps such policy was inspired by oft-cited success stories like Kenya, which leveraged mobile/electronic money transfer schemes to drive financial inclusion (see Safaricom's M-Pesa Programme);[2] as well as China, which leveraged the network benefits of digital and online platforms (example Alibaba and Tencent) to propel digital transactions. A common lesson from these experiences is that digital financial solutions have a high degree of scalability, and are especially effective in reaching the last mile in rural/remote areas. They reduce information asymmetries toward credit assessment and transaction costs in serving the low-income demographics.[3]

The prominence of India's financial inclusion efforts is reflected by the increased traction of flagship government schemes such as the Pradhan Mantri Jan Dhan Yojana (PMJDY) and the promotion of the affiliated JAM Trinity. Such policy impetus has certainly helped push the needle as the volume of digital transactions rose by approximately 89.5 percent during FY 2017-18.[4] Moreover, with around 493.96 million internet users,[5] the world's second largest smartphone marketplace, and around 1.18 billion wireless users,[6] India's digital payments ecosystem is poised to becoming a US$ 1-trillion proposition by 2023.[7]

To realise such value, policy frameworks should appropriately address the twin objectives of adoption and ecosystem integrity. Regarding the former, engendering competition, innovation and an overarching level playing field between banking and non-banking counterparts are increasingly considered as prerequisites. To this end, India is overhauling its current legal framework, i.e., the Payment and Settlement Systems (PSS) Act, 2007. The thrust of this reform is on achieving the above imperatives whilst balancing them with monetary policy considerations.

This article focuses on ecosystem integrity through the prism of cybersecurity of digital payments. This is because trust in the digital financial ecosystem for first-generation internet users acquainting themselves with new digital mediums is important as insecurity directly contributes to the failure of such digitisation efforts. It is equally important that security frameworks are carefully crafted to avoid contradicting aspirations of adoption and inclusion. The article attempts to rationalise these sometimes opposing considerations, and proposes legal and policy recommendations.

Market Characteristics

Digital payments include both "online" and "mobile" payment and settlement systems. [8] Major payment channels in India include the following:

- Interbank card (both debit and credit) networks;

- Large value transfer systems (LVTS) i.e. National Electronic Fund Transfer (NEFT) and Real Time Gross Settlement (RTGS);

- Retail payment systems like the Immediate Payments Service (IMPS) and Unified Payments Interface (UPI);

- Internet Banking, Mobile Banking, Unstructured Supplementary Service Data (USSD); and

- Prepaid Payment Instruments (PPIs) commonly referred to as "mobile wallets": stored value accounts which have become popular mediums for low-value transaction activities.

Simultaneously, security frameworks should remain cognisant of the two-sided nature of digital payments. The major actors from the demand side include merchants and consumers. It is, however, from the supply side where the multiplicity of actors becomes more evident. The range of market participants in India includes:

- Reserve Bank of India (RBI): India's sole provider of LVTS systems and related infrastructure;

- National Payments Corporation of India (NPCI): India's sole/umbrella retail payments system/infrastructure provider;

- Intermediate Payment Service Providers (PSPs) & Switch Providers: Include Banks; Payment Banks; Mobile Wallet Companies; Online Payment Gateway Service Providers; and Card Network Companies;

- Physical Infrastructure Providers: ATM Operators; Point-of-Sale (PoS) terminal and mobile device providers

- Other Participants: Third-Party Vendors & Network/Connectivity Providers

Such disaggregated value chains with disparate actors of varying scale and size, afford discrete vector points that malicious actors can potentially exploit. Moreover, this mushrooming of parties managing financial data adds to the complexity of financial networks. Lauer & Lyman (2015) argue that this increases privacy and security risks. [9]

Anatomy of Cyber Vulnerabilities

A recent study found that data breaches occur in India at a rate surpassing the global average.[10] In this context, given that digital financial networks are inherently complex comprising several nodes, firm-level information security operations are often inadequate and can be undercut by the actions of other parties within the same network.

Major incidents that demonstrate such systemic insecurities include the Hitachi ATM switch server data breach reported in October 2016 wherein a prolonged unpatched vulnerability led to the compromise of around 2.9 million Indian debit cards;[11] and a UPI application layer bug which cost customers of the Bank of Maharashtra[12] around INR 250 million which was reported by the press in March 2017.[13] Even globally, the data breach involving American credit institution Equifax[14] disclosed in September 2017 illustrates the scale of attacks targeting large financial data ecosystems. On a related note, security analytics experts Symantec find that poor user security/password practices increase likelihood of cybercrime and undermine otherwise robust cybersecurity measures at the hardware, software and network levels.[15]

Moreover, when looking at electronic payments frameworks, the International Financial Consumer Protection Organisation observes that the systems in countries like Brazil, Canada and Japan are susceptible to the risks of identity theft and fraud.[16] Similarly, India's digital payments ecosystem has also been plagued by continual increase in "cyber fraud".[17] Other common cyber threats afflicting digital payments ecosystems include malware installations, phishing attacks, SIM Card Swap Attacks, and unreliable devices and infrastructure.

Indeed, the capabilities of malicious actors continue to expand due to the invariable leaks of exploits developed by governments for cyber offensive capabilities. Such leaks lead to the creation and proliferation of widespread attacks that can target either specific systems or wider global computer systems, infrastructure, and networks. For example, the EternalBlue exploit developed by the United States' nodal National Security Agency (NSA), was leaked by the "Shadow Brokers" hacker group.[18] This exploit was ultimately leveraged by state actors (North Korean and Russian) to spread the WannaCry ransomware (May 2017)[19] and NotPetya cyber-attack (June 2017)[20] which affected systems across multiple jurisdictions. Pertinently, India was one of the worst-hit countries by WannaCry with over 40 thousand affected computers.[21]

The Fallacy of the Cybersecurity Silver Bullet

The above analysis demonstrates the fragility of cyberspace. It also points to the dynamism of cyber threats—that it is impossible to completely secure technology markets, especially through specific regulatory prescriptions. Therefore, legal frameworks should be considered as an essential cog in an ecosystem's cyber resilience machinery which remains considerate of the post cyber-attack paradigm.

Remaining mindful of such limitations, the rest of this article proposes a way forward for India's policymakers—a way forward that informs itself through commonly accepted international strategies. Specifically, it attempts to arrive at common principles for future laws that can adequately limit the underlying risks[22] in strategically and economically critical ecosystems like India's digital financial networks.

Risk-Based Regulation: Guiding Principles

It is essential for frameworks aiming to secure digital financial ecosystems to address two basic requirements. First, there is a need to conceptualise appropriate risk weighted approaches to ensure confidentiality, integrity and availability for major payment systems. These principles form the bedrock of information security. Drawing inspiration from the European Union's Article 29 Working Group on Data Protection,[23] these principles can be defined as follows:

'Confidentiality': unauthorised access or accidental disclosure of information;

'Integrity': the alteration of systems to create system vulnerabilities; and

'Availability': the accidental loss or unavailability of access to information systems and the information within.

Second, such sector-specific conversations need to be appropriately rationalised with law-making efforts in sector agnostic technology arenas. For example, in August 2017, a nine-judge bench of the Supreme Court confirmed an individual's right to privacy as a fundamental right under the Indian Constitution. The Court also categorically declared 'informational privacy' (relevant for internet/data economies) as a key constituent of this umbrella right.[24] Pursuant to this, the Indian government is undertaking a process to create a comprehensive data protection bill, and recently published the "Personal Data Protection Bill, 2018". Although designed primarily through the lens of user-privacy, key provisions also govern how payment and settlement system providers operate vis-à-vis cyber/information security.

The following sections analyse India's (1) payments specific and (2) general legal frameworks and analyses international practices to propose recommendations.

1. India's Payments and Settlement Regulatory Framework

The primary legislation governing digital payments in India is the 2007 PSS Act. The objective of this Act was to designate the RBI as the supervisory and regulatory authority for payments and settlement.[25] This Act came into force in August 2008 in an era where digital financial inclusion was in its infancy and its intention was to provide a legal basis for netting and settlement finality. However, various government committees looking into the financial sector have advocated for reforms. In December 2016, one such committee report recommended that laws on digital payments should adopt risk-based approaches which, inter alia, also guide safety and security requirements.[26] Taking this forward, the ongoing overhaul of the framework via the Payment and Settlement Systems Bill 2018 is expected to adopt a risk-based framework that will require regulatory requirements to consider data security risk, settlement risk, operational risk and business risks arising from particular entities or ecosystems. Moreover, in order to foster legal clarity, the proposed law aims to consolidate the framework and reduce the number of legal instruments applicable for payments ecosystem participants. The law is expected to marry these guiding principles with the principle of technological neutrality to promote innovation within the ecosystem.

As such, a reform is sure to implicate security of future payments ecosystems, previous information security efforts are instructive through four distinctive prisms—as articulated in Table 1.

Category	Approach of RBI
Organisational Control Requirements	Broadly, both banks[27] and PPIs[28] are prescribed specific cybersecurity objectives like incident response, risk management and recovery. The legal instruments/frameworks nevertheless remain prescriptive and mandate banks to adopt baseline organisational security requirements including internal cybersecurity policies, a central security operations centre for threat detection, a bank wide cyber crisis management plan, network security protocols with firewalls and other perimeter defence strategies.

Category	Approach of RBI
Transaction, Infrastructure and Instrument Security	Transaction security is largely achieved through the process of authentication wherein payment system providers deploy technological protocols to verify that the person who initiates payment and settlement requests is in fact the individual undertaking the transaction, and not another unconnected party. Having analysed the RBI's requirements for mobile-banking,[29] card-led transactions,[30] PPI-led payments, the approach is largely prescriptive and mandates organisations to undertake technologically specific security measures. Such measures broadly encompass PIN/OTP-based two factor authentication (2FA) requirements, transaction limits and velocity checks, fraud and AML checks, and maximum number of invalid access attempts and suitable timeout features. At the same time, such measures can stymie user adoption and increase transaction failure rates. Thus, the RBI has tried to relax 2FA requirements for low-value (less than INR 2 thousand) card-led transactions online. Alternatively, at the infrastructure (ATM & PoS), and the instrument (card and application) levels, requirements are prescribed based on standards developed at internationally endorsed standard-setting industry groups like EMVCo and the Payments Card Industry-Security Standards Council (PCI-SSC).
Know-Your-Customer (KYC)	All authorised payment system providers (banks, PPIs, PSPs, etc.) are directed to comply with identity verification/KYC requirement as outlined in RBI regulations.[31] They are tools to prevent money laundering operations and are an important component of anti-fraud detection. However, excessive or escalation of identity verification requirements has been observed to stifle volume of adoption and conflict with financial inclusion aspirations.[32] Additionally, efforts to leverage India's national identity database, i.e., Aadhaar as an instrument of interoperable and large-scale KYC[33] has been hit with privacy concerns and previously been challenged in India's Supreme Court.[34]
NPCI	India's sole retail payments system/infrastructure operator the NPCI's bouquet of offerings, inter alia, includes the UPI (an application layer built over India Stack[35]). The NPCI sets specific security standards for PSPs to access its interoperable payment systems.[36] Nevertheless, since it occupies such a central role in India's payments landscape there is a need to highlight that NPCI systems have been susceptible to security incidents (see Bank of Maharashtra incident). Additionally, research by Privacy International also clearly expresses the invasive nature of UPI's architecture which centralises data concentration and opens up user-financial data to indiscriminate data-harvesting/mishandling.[37] Scholars like Acharya argue that UPI lacks appropriate consent, and collection/processing/purpose limitation safeguards.[38] Such privacy and security challenges exemplify the inherent risks of single-player retail payments infrastructure/system operator markets; especially one with such large-scale roll-out responsibilities. This leads to an erosion of trust, and casts doubts on the integrity of a payments ecosystem which can deter overall adoption rates. A government committee report recently recommended that markets require realignment to eliminate such glaring institutional risks of single point of failure.[39]

Embedding Risk-Based Strategies for India's Digital Financial Security

As analysed above, RBI regulations and standards have so far been inclined toward prescription as opposed to principles. However, as the transition toward a more principled risk-based, technologically neutral legal regime begins, it is essential that security requirements are reconfigured appropriately. Such reform should ideally learn from international precedents that will be discussed in the next sections of this article.

Organisational Security: Risk management strategies at the organisation level require solving for: a) risk assessment including identification, analysis, and evaluation, and regular stress-tests; (b) risk treatment including adequate security measures (periodically updated through activity lifecycle); and (c) preparedness/ continuity plans including prevention, detection, response and recovery with effective escalation protocols. Specific to electronic payments, this should also comprise incident monitoring and reporting; risk control and mitigation; transaction traceability; customer identification and strong authentication; transaction monitoring; protection of sensitive transaction data; and end user education.

According to groups like the Organisation for Economic Cooperation and Development (OECD),[40] European Union Agency for Network and Information Security (ENISA),[41] and the Group of Seven (G7),[42] as well as financial authorities like the Bank of International Settlements (BIS),[43] compliance regimes should be designed with appropriate flexibility (avoiding stating "how"). Such an approach allows an organisation to evaluate the degree of risk associated with a certain activity/type of network and nudged toward fulfilling commonly accepted principles of risk management dynamically. To achieve this, policies are recommended to create incentives towards internationally endorsed IT governance standards like ISO 27001 and 22301, and for robust supply chain security (ISO 28000), as operations are being increasingly outsourced to third-party vendors.[44]

To this end, a special focus group on digital financial services (DFS) under the International Telecommunications Union (ITU) has consultatively developed security standards best practices specific to the sector, building on earlier standards of the EMVCo and the US' National Institute of Standards and Technology (NIST). The following are the key principles under this:

- Access Control (Principle of least privilege);
- Authentication;
- Non-Repudiation (to assure particular actions have taken place);
- Confidentiality (Encryption via cryptography);
- Security of Communications;
- Data Integrity (Integrity Monitoring Tools);
- Availability (Firewalls and Intrusion Detection Systems); and
- Privacy (Preventing Unauthorised Access)

Risk-Based Transaction Security: India's current reliance on OTP-based 2FA protocols for digital payments requires revisiting. This is because it has proven to be a stumbling block for onboarding bottom of the pyramid demographics. Moreover, groups like NIST have acknowledged that SMS-led authentication makes users vulnerable to social-engineering and technical security threats.[45] To adequately address such challenges, frameworks in jurisdictions like Austria, Brazil, and Singapore have shifted toward technologically neutral frameworks.[46] Pertinently, the European Union's (EU's) Revised Payment Services Directive (PSD2) has adopted a Strong Customer Authentication (SCA) regime based on factors of knowledge, possession and inherence. Here again a risk-based, technologically neutral approach has been adopted, wherein lower-risk transactions[47] can be afforded more lenient authentication standards and exemptions. In response to such headwinds the EMVCo group is developing risk-based SCA standards to balance security principles with user convenience considerations. In October 2016 it launched its 3D Secure 2.0 specification which analyses device offered data and leverages it with biometric innovations to offer a layered Risk Based Authentication standard.[48]

Principles for KYC Verification: Target 16.9 of the UN's Sustainable Development Goals calls for "legal identity for all"[49] especially for access to financial services.[50] In this context, the ITU's DFS focus group observes that rigid identity verification processes can conflict with financial inclusion targets. To this end, regulators are advised to adopt risk-based frameworks where required Levels of Assurance (LOA) are raised proportionately (ISO/IEC 29115). The benefits of a dynamic risk-based approach are that it reduces friction to financial onboarding, and as new (riskier) services are requested KYC requirements are escalated equitably.[51]

At the same time, policymakers should be cognisant of emergent innovations with respect to secure, interoperable and consequently scalable identity verification practices. For example, expert groups like the ITU are proponents of Federated Digital Identity Management marketplaces.[52] A key benefit associated with such frameworks is the limitation of privacy concerns. Such management systems limit the number of entities and instances where personal data is shared by users. Once verified, other service providers can onboard/verify the identity of customers on the basis of corresponding tokenised information, limiting access to sensitive personal information. The US' NIST has recognised Federated Identity Management as a privacy-respecting and interoperable security best practice and has established a Trusted Identities Group to promote its adoption within identity verification ecosystems.[53] Further, NIST has released Digital Identity Guidelines (June 2017) which, inter alia, strives to standardise Federated Identity Architectures. These standards also provide industry guidance on privacy-enhancing techniques to share tokenised KYC related information.[54]

Additionally, regarding linking of different accounts (like bank accounts) to a national identity, Austria's Citizen Card[55] framework has been cited as a privacy-respecting best practice. Here, this card comprises multiple sector-specific accounts, derived from the nodal national identity number. Pertinently, each identity account is individually protected through requisite cryptography. This helps limits profiling risks, and enabling revocation and replacement of encrypted identifiers in the event of breaches.[56]

Resolving Single Point of Failure Risks: Financial authorities like the BIS, Bank of England and the European Central Bank (ECB),[57] hold that it is incumbent on

regulators to resolve institutional risks single points of failure in retail payments market, whose disruption can have wider ramifications across ecosystems.[58] In separate findings, the ECB opines that disruptions in non-substitutable systems increase trading frictions,[59] and may drive users to use other channels like cash.

2. Rationalising with General Data Protection/Security Conversations

Section 43A of the Information Technology Act (IT Act) read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 outline information security and data protection requirements for all business handling SPDI including "credit card, debit card, and other payment instrument details".[60] The rules require businesses to implement specific protocols to collect, process, transfer and disclose SPDI and also mandates implementing information security policies risk proportionate security controls, risk management protocols (informed by ISO/IEC 27001 standards), and annual cyber audits.[61] Enacted in an era when the law was introduced to cater to the interests of the BPO sector,[62] the SPDI framework has drawn criticism due to the lack of a discernible redressal mechanism and negligible enforcement with only 17 judgements and none since 2011.[63]

Proposed Data Protection Bill

Owing to its legacy basis, criticisms of negligible enforcement, and the Supreme Court's decision regarding informational privacy as a fundamental right, both the Indian government and judiciary agreed on the need for a comprehensive data protection framework. To this end, the SPDI framework is under the process of being replaced by a new "Personal Data Protection Bill". Although not its primary purpose, the proposed framework is set to directly implicate India's information/cyber security landscape. Admittedly, the Bill's current draft raises various concerns such as its highly restrictive treatment of cross-border data flows/data localisation[64] and arising cybersecurity challenges from geographic single point of failure risks. This section of the article limits its analysis to the Bill's impact on transaction security.

If enacted, the Bill will govern all "processing of personal data"[65] and the relationship between users ('data principals') and entities that determine the manner of personal data[66] processing ('data fiduciaries'). Critically, it is the Bill's definition and grounds of processing of "sensitive personal data"[67] which breeds concern. Specifically, "financial data" is a constituent of this special category of personal data and includes account details, card or payment instrument details, or any data that reveals the nature of relationship between a data principal and a financial institution including financial status or credit history.[68]

. This is important because under the Bill , the grounds of processing for sensitive personal data (including card and payment instrument data) requires explicit consent from the data principal which must satisfy being informed, clear and specific[69]. Critically, "reasonable purpose" exceptions to the informed consent standard for processing most personal data would not be extended to financial data. This means that data fiduciaries would not be allowed to dynamically process financial data without "explicit consent" for, inter alia, fraud detection;

and network and information security purposes. Such standards will directly affect transaction velocity and monitoring systems often deployed by payment service providers to secure its networks real time through dynamic fraud checks; typically leveraged for strong risk-based authentication.

Critically, the Bill and the BN Srikrishna Committee recommendations hold that in case of any conflict between this law and other sectoral laws, the provisions of the Personal Data Protection should always prevail. In this context, the committee highlights that the PSS Act 2007 (among 50 laws) may require amendments to conform to future data protection standards possibly affecting future information/ cyber security policy for digital payments.

Reconciling Data Protection Laws with Transaction Security

When juxtaposed vis-à-vis international practices, the Bill's treatment of financial data warrants scrutiny. Australia's "Privacy Act", for example, leaves financial information outside the framework's scope of its SPD equivalent i.e. "sensitive information". Rationale offered by the Australian Law Reform Commission for such categorisation is that financial information, unlike other categories of sensitive information,does not reveal physical attributes or personal beliefs and moreover, financial institutions have a legitimate interest in processing such information.[70] Similarly, the UK's Information Commissioner's Office (ICO) leaves financial data outside the scope of its "special category data".[71] More generally, the Annexure to a dissent to the BN Srikrishna Committee's report outlines just one out of 68 cited jurisdictions studied characterise financial data under the ambit of sensitive personal data equivalent categories.[72]

Nevertheless, even if Indian lawmakers deem that users' financial data deserves special privacy protections which deviate from international standards, such protections should not come at the cost of requirements that compromise the integrity of financial systems and related networks. Finally, it is advisable that data protection laws avoid a catch-all provision which states that requirements under the Personal Data Protection Bill supersede other sectoral requirements– as it can lead to absurd consequences. This is especially so given that the Section 12(5) should a data principal withdraw consent for processing of any personal data then all arising legal consequences shall be borne by the principal itself. Such legislative construction can lead to adverse situations that compromise network integrity and potentially leave consumers without adequate redressal. There is thus a need for nuanced government responses that reconcile user privacy laws with cybersecurity imperatives.

In this context, principle-centric cybersecurity frameworks for a sector like digital payments, which necessitate risk-based strategies are harmoniously integrated within core regulatory regimes governing the space, and adequately rationalised under new legal regimes related to privacy conversations. As usual, the answers are not easy, and demands comprehensive multistakeholder discourse before a final enactment.

11 Lessons from the Fight against Digital 'Influence Operations'

Stephanie MacLellan

The Russian interference in the 2016 elections in the US has been widely reported and analysed. Intelligence agencies and tech companies have found false social media accounts, groups and event listings that have been set up to imitate Americans on either side of the political divide, producing disinformation and highly charged rhetoric at an alarming rate.

However, so-called "influence operations" like these did not stop with the election of Donald Trump to the US presidency. Elections in multiple countries, including the Netherlands and France in spring 2017, were accompanied by signs of Russian attempts at interference or disinformation.[1] In the US, security researchers this year found hundreds of social media disinformation accounts linked to Russia and Iran, many of which did not appear to be directly tied to either the 2016 polls or the 2018 midterm campaigns.[2]

The US Department of Justice describes influence operations, also known as "information operations," as "covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives."[3] However, the specific objectives of influence campaigns may vary. During an election, they may promote one candidate over another; they are just as likely to spread confusion, discord and distrust in the entire process. They may discourage certain groups of voters from going to the polls, drown out or undermine legitimate journalism with false reports, or convince citizens that the election results should not be trusted due to voter fraud or other illegal activities.

The digital nature of today's disinformation campaigns makes them especially difficult to counter. Because of the global nature of the internet, they can be launched from anywhere in the world. Perpetrators can use digital tools to mask their location, making it more difficult to identify them. To begin with, many of these techniques rely on social networks, which are run by private companies that may be reluctant to allow public oversight into the proprietary mechanisms that determine which content appears on their platforms.

These technical challenges combine with broader global governance challenges – such as underdeveloped norms around how states should deal with online interference short of acts of war, and the recognition of freedom of expression as

a human right – to make this a particularly vexing dilemma. However, a growing body of research into digital influence operations, as well as the experiences of states that have held elections since 2016, have uncovered some policy options that show potential for limiting the effect of these campaigns.

Whole-of-government approaches

Russia's digital influence operations to date have been characterised by a "scattershot" approach. Rather than one consistent, coherent narrative that can be countered, they have promoted a smorgasbord of opinions on hot-button topics using a variety of methods, from planning events on Facebook, to high-volume automated postings on Twitter, to releasing sensitive information hacked from political operatives' accounts. "The nature of IO [information operations] deliberately makes it difficult for one entity or group to possess the technical expertise and subject matter knowledge to attribute and refute attacks and decide what constitutes an information operation and what does not. . . . This means that the analysis to piece together IO puzzles will rely on collaboration and co-operation across sectors and party political lines."[4]

Influence operations and other forms of election interference may fall under the jurisdiction of several government agencies working in security, intelligence, foreign policy and other areas, as well as election bodies at various levels of government. These agencies will need to work together to share threat information, strategise and respond, and it is considered good practice to appoint a lead agency to coordinate them.[5] For instance, in Sweden, the government has brought together four key agencies to cooperate on election intelligence and strategy, led by the Civil Contingencies Agency (MSB) that is normally in charge of emergency preparedness.[6] The MSB also trained more than 10,000 civil servants and election officials on how to detect and respond to influence operations.[7] As with other emergency preparedness activities, running tests and scenario exercises ahead of time will allow the relevant agencies to clarify their roles and identify vulnerabilities before they are faced with active influence operations.[8] At the same time, establishing clear protocols well ahead of an election will make it less likely that a response to influence operations will become politicised – or even to appear politicised, which can be equally damaging.

Any government strategy should also involve strong public statements against influence operations, which can serve two purposes: first, to encourage public vigilance; and second, to shift the cost-benefit analysis of rival states as they consider launching influence operations. Observers note that after senior leaders in Germany and Sweden issued strong, consistent warnings that there would be consequences for any state that meddled in their elections, there were no signs of Russian interference affecting either outcome.[9],[10] On the other hand, in the wake of contradictory and equivocal statements from the US administration about election interference, influence operations have continued on social media. "In some ways, the United States has broadcast to the world that it doesn't take these issues seriously and that any perpetrators of information warfare against the West will get, at most, a slap on the wrist," wrote Facebook's former head of security, Alex Stamos.[11]

Working with technology companies

Any efforts to stop influence operations will need to involve the very same digital platforms that serve as venues for much of this activity. In the past year, three of the biggest tech companies – Google, Facebook and Twitter – have rolled out enhanced transparency measures and other restrictions for political advertising on their platforms.[12],[13,14], Advertising restrictions, however, do not affect unpaid content, which can be just as effective in reaching audiences, if not more. The focus on social media giants also leaves out other players, such as the digital advertising industry and instant messaging platforms such as WhatsApp.

Issues like these are at the core of the debate around regulating digital platforms. Critics have questioned whether relying on platforms to police themselves puts too much power in the hands of private companies to rule on sensitive and complicated issues such as freedom of expression. Instead of removing questionable content, one alternative approach gaining traction focuses on transparency – such as identifying automated accounts or presenting alternative sources of information – to help audiences make their own judgments on the legitimacy of the content they see.

In any case, there is a clear need for more research into the interaction of influence operations and digital platforms, which will help platforms and policy-makers determine the effects of various interventions. Social media giants collect troves of data that could be used for this purpose; making this data available to researchers, while shielding user privacy, would have benefits for democracy while also helping the companies convince their users that they can be trusted to weed out bad actors.

Public education and awareness

Public education may be the strongest defence against influence operations, because it does not depend on the cooperation of specific social networks, which can always be displaced from their dominant positions by emerging competitors. Nor does it put governments or private companies in the difficult position of weighing in on the limits to freedom of expression. Instead, the goal is to build "societal resilience" against influence operations.[15]

Telling the public about attempted influence operations can be helpful in itself by allowing people to consider the source of the information that they consume and share. For instance, when hacked information from Emmanuel Macron's campaign was released on the eve of the French election in April 2017, his team immediately announced what had happened and said that some of the leaked material was fake. This helped mitigate the damage by discrediting the leakers.[16] Earlier this year, the US Department of Justice established a policy to guide how and when it would tell the public about influence operations targeting elections. "When people are aware of the true sponsor [of information], they can make better-informed decisions," Deputy Attorney General Rod Rosenstein said.[17]

These disclosure efforts should be complemented by media literacy initiatives that help citizens think more critically about information disseminated in social media. In countries where election interference was not successful, such as France and Sweden, trust in traditional media remains high while information shared through

social media is more likely to be treated with skepticism.[18],[19] This is not to say that digital news should be disparaged across the board, but that helping people learn what makes information trustworthy may help limit the effectiveness of online disinformation.

Another effective strategy may be explaining the mechanisms behind influence campaigns to demonstrate how they spread their messages, rather than focusing on the content of the messages.[20] A similar approach to media literacy has been used with success in post-conflict peacebuilding in Central Africa. When a radio soap opera was developed to inform listeners about the psychology of propaganda that incites hatred, its listeners were found to be more likely to think for themselves.[21] This kind of information may help build resilience to disinformation messages that play on audience emotions by teaching them to recognise how they work.

Media literacy initiatives will not realistically have an immediate effect, especially in polarised environments such as the United States where certain segments of the population have been primed to disregard challenging viewpoints as "fake news." Yet, various examples from the fields of public health and safety – such as wearing seatbelts, or not bringing liquids during air travel – show that it is possible to adapt public behaviour over time; key is to educate the public that there is a benefit to adapting.

While this article has focused on election-related influence operations, it is important to remember that these campaigns can and do happen at any time – as seen in the social media posts linked to Iran and Russia that continued to appear long after the 2016 US campaign was over. Influence operations also have the potential to create a security crisis – for instance, by targeting the financial sector or spreading rumours of an impending disaster. Policy-makers should look at their vulnerabilities beyond the election cycle and prepare accordingly.

Indeed, this is an emerging field. In a rapidly changing global online ecosystem, there is still much to learn about how digital influence operations work and how they can be effectively countered. There is also an opportunity for the international community to share information on threats as well as lessons learned from their own experiences. While each country will have to adapt its approach for its own government structures and cultural environment, this growing body of expertise and experience means there is no need to start from scratch every time.

12 A 21-Century Social Contract: Are We Asking the Right Questions?

Mihir S.Sharma

In a digital world work, governance and rights will all be radically different than they are now. The systems and structures built up over the course of the twentieth century to link governments, companies, workers and consumers will come under increasing amounts of stress; if they are not to buckle, causing dislocations and divisions that will threaten economic interdependence and state security, then they must change and be changed in tandem with technology.

Automation, artificial intelligence and digitalisation are processes of technological change that regulation might be able to temporarily constrain, but will be unable to wholly reverse. Each of these will have a different disruptive effect on inequality, employment, and the state. Large-scale mass manufacturing might soon become obsolete in certain sectors; already new factories in higher-technology sectors are capital-intensive at the cost of the number of people employed. This is true even in relatively low-wage countries like India, indicating that there has been a fundamental shift in the production function at the cost of labour. "Jobs for life" are becoming rarer and rarer outside the public sector – one reason, perhaps, that government jobs are once again becoming a preferred destination for those with fewer skills and lower levels of education. The AI and machine learning revolution is not so far along; but it puts at risk middle-level white-collar jobs. Thus, for the first time in history, the educated middle class might also be at risk from technological change, and not just blue-collar workers.

The existing model of welfare and employment is insufficient to deal with these changes. It is predicated on several assumptions: that employment status is a binary, for example. You are supposed to be either in a job, or out of it. If you are in one, then it is your employer's responsibility to contribute to your healthcare and your pension fund. If you are out of a job, then in many countries it is the state's responsibility to assist you to find another one. Minimum-wage law is structured to ensure that those working regular jobs at regular times earn enough to live. Meanwhile, trade unions create the possibility of collective bargaining between a company and its current workforce, which is a clearly defined set of individuals with broadly similar interests. Governments act as referees between all these interest groups and also rely on workers and companies for revenue.

This model, the twentieth-century consensus, will endure multiple points of breakage as technological change intensifies. Employment is, for one, no longer binary. In the "gig economy", people can choose multiple forms of income-generating activity. Is an uber driver "employed"? Courts and regulators are

constantly asked to pronounce on that and similar questions. The differing answers should reveal that we are in fact asking the wrong question. A twenty-first century activity is being constrained by lines drawn in the twentieth. Regulations and legal systems will have to accept that individuals can now no longer be easily segmented into workers, employers, contractors, capital-owners, and so on. Each and every individual will be, in the future, some combination of these. Economic activity matters, not economic identity.

Thus a new form of social protection, adapted to these fluid identities, is required. In some sense, the world is catching up with India. This country has long struggled to provide a social safety net within an economy without large-scale manufacturing and in which formal employment was hard to come by. What the rest of the world calls "the gig economy" we have long just called "poverty". There is much to be learned from the attempts in countries with large informal sectors to provide to their citizens an approximation, however rough, of the benefits accruing to formal-sector workers in more advanced economies.

Other aspects of state activity will also need to change. Increasingly, "infrastructure" will not just mean large-scale physical plants like highways, ports and power stations. Social networks, peer-to-peer communication systems, payment technologies and others will perform an infrastructure-like service: they will be the backbone upon which productive activity and livelihoods depend. But can these be paid for or provided by the state, as was some of the infrastructure that powered previous industrial revolutions? Almost certainly not. In other words, private companies will inevitably take over the duty of providing such quasi-public goods. Will they be treated like regular companies? Distrusted, broken up or regulated as monopolies? Be the subject of attempted nationalisations? There are no easy answers to this question. But it is important to understand that, once again, disputes between companies like Google and authorities like the European Union indicate that we are trying to answer the wrong questions. The question is not: Is Google behaving like a regular company? Instead, we should accept that such networks and providers are part-utility, part-infrastructure, and part-company. Again, we must break free of the tyranny of economic identity if we are to properly regulate and encourage economic activity.

What, thus, can serve as a new social contract between individuals, companies and the state that both protects individual interests and promotes economic dynamism? And who will stand guarantor to that contract? The problem is that the relationships that define governance in the digital economy are evolving so quickly that no single agent or actor seems able to perform this task. Instead, it must be the purpose of politics and policy to evolve norms that will underpin a rights-based, equitable and growth-oriented digital economy — one that focuses on activity, and not identity.

The specific nature of what these norms are can still be debated, although researchers at the Observer Research Foundation have already identified some possibilities. However, what is undeniable is that the political process needed to evolve these norms will need not just different assumptions but also different actors than those currently in evidence. Trade unions, chambers of commerce,

class-based political parties are all struggling to retain their relevance in the twenty-first century economy. When workers, shareholders, and entrepreneurs are so diffuse, heterogenous and atomised then who can speak for them as a collective? Particularly when so many individuals are, in effect, all three at once?

The first task towards constructing the right norms that could underpin a 21st-century economy is, therefore, to evolve the right participants for it. Individuals will have to be canvassed, enlisted and organised as participants in this public conversation both as consumers and as workers, both as capital-owners and as citizens. Different bodies will need to represent them in each case, and allow for an open negotiation between the various interests that are embodied in both the body politic and the individual. This is not an easy task – restructuring political engagement never is – but it is one that is essential. To this end, both government policy and private sector actions must actively seek to create co-operative networks for these various participants in the digital economy. The individualisation of labour cannot be allowed to derail the chance to construct a 21st-century economy that can work for everybody.

13 Gig Economy, Women, and the Future of Work

Vidisha Mishra

Technology is changing the world of work. While policy discourse and commercial interventions focus on the positive impacts of ongoing digital transformations on women's participation in the labour market – evidence indicates a mixed picture.

The gig economy or the emerging labour market characterized by the prevalence of short-term contracts or freelance work is credited with enabling more women to work due to it's inherent flexibility which lets them combine paid work with caring responsibilities -- which is still disproportionately carried out by women. Further, technology-enabled gig work, or platform work, is believed to be beneficial to women as they can provide work opportunities for women in contexts where their participation in the formal economy is restricted by socio-cultural barriers.

For India, with just 27 per cent of women participating in the labour force, compared to 79 per cent of men, the gig economy could be advantageous. The emergence of the tech-enabled gig economy presents the opportunity to reimagine traditional worker-employer relationships from a gender lens. At the same time, studies indicate that men have the upper hand in the absence of rigid rules, and existing gaps are easily replicated in alternative work models. It is important to question the long-term consequences of non-standard forms of work. While women could benefit from flexibility – these benefits could be offset by increased precarity, reduced job quality, and reinforced gender stereotypes.

The impact of the gig economy is context-specific

Recent research by the Overseas Development institute finds that unlike in the US and Europe where the gig economy is already mainly technology-enabled, in India, while technology-enabled, individual-driven gig work is growing -- companies also sign up workers from low-income areas for face to face visits. These workers are not classified as full-time employees but rather as 'independent contractors' who deliver services to clients facilitated by the platform. This is particularly true for female domestic workers connected through on-demand platforms. In such contexts where women are disproportionately represented in the informal and unregulated economy, gig work can actually worsen worker rights and result in backtracking on hard-won rights and benefits.[5]

Existing gender gaps are replicated

Further, the gig economy, like the traditional economy, is not independent from persisting social conditioning and gender-biased socio-cultural norms. For

instance, a study by Stanford, University of Chicago and Uber, drawing on evidence from a million rideshare drivers on Uber, estimated that on average, men earn approximately 7 percent more than women. The reasons behind this were found to be: men driving at higher speeds, men accumulating more experience, and the different choices across genders over where they were willing to drive.[6]

Further, while it is true that platform work could reduce barriers to entry for women, particularly in male-dominated industries like taxi services, another study found that while more than half of online platform participants quit within a year, women were more likely to drop out than men.[7] Till the structures that influence existing issues such as the gender pay gap, confidence gap, gender-based occupational segregation, and biases in hiring are not addressed – these issues are likely to be replicated in the gig economy.

Flexibility and unpaid work

Globally, women do over 76 percent of all unpaid work, with that proportion rising even higher in India where women do 90 percent of housework. Extant research establishes an inverse link between the amount of time spent by women and girls on unpaid care work and their economic empowerment.[8] While there is evidence to suggest that grater work flexibility results in higher employment rates among mothers, the possibility that this flexibility could reinforce the idea of women being the primary providers of care and unpaid work, while also increasing their paid labour, cannot be negated.

While in the future, technological innovation could automate the burden of care work, this would require first recognizing the value of women's unpaid care work and unpaid work in general, and then investing in these assistive innovations. Until care and unpaid work are recognized, reduced, and redistributed, the flexibility afforded by the gig economy could be more burdening than empowering. In addition, it is important to acknowledge the difference between building in flexibility into full-time employment and the unsteady flexibility of the gig economy.

Women and the gig economy in India

The Observer Research Foundation and the World Economic Forum collaboratively conducted a survey of more than 5,764 Indian youth to generate insights on the nature of youth aspirations with respect to skills, jobs and work.[10]

Findings from the Youth Aspirations in India Survey reveal that young Indian women are cautiously optimistic about the gig economy. While 17 percent of women were very interested in participating in the gig economy for their main source of income, 35 percent reported being not interested. In comparison, while 20 percent of all female respondents reported being very interested in participating in the gig economy to supplement their main source of income, 31 percent reported being not interested.

The survey indicates that at present, there are more young women not interested in the gig economy than women who are very interested. At the same time, 37 percent of women reported being moderately interested in participating in the gig economy to supplement their income, and 36 percent reported being moderately interested in participating in it for their main source of income -- indicating cautious openness.

Figure 1: How interested would you be in participating in the gig-economy to supplement your income?

How interested would you be in participating in the gig-economy to supplement your income? (%)

Gender	Very interested	Moderately interested	Not interested	Can't say
Male	29	37	23	10
Female	20	37	31	11
Non - Binary	6	38	50	6
Total	26	37	26	11

Figure 2: How interested would you be in participating in the gig-economy for your main source of income?

How interested would you be in participating in the gig-economy for your main source of income? (%)

Gender	Very interested	Moderately interested	Not interested	Can't say
Male	26	37	26	10
Female	17	36	35	12
Non - Binary	6	31	50	13
Total	23	36	30	11

The female respondents who were very interested or moderately interested in participating in the gig economy reported the flexibility in hours and schedule as the main reason for wanting to do so; this was followed by greater decision-making powers.

Figure 3: Why would you want to be a part of the gig economy?

Why would you want to be a part of the gig economy? (%)

Gender	Flexibility in hours and schedule	Unlimited configurations in pay	Variety in work	Self employment/greater decision-making powers	Changing attitudes towards freelancing
Male	32	12	19	27	9
Female	31	8	20	26	15
Non-Binary	33	17	0	33	17
Total	32	11	19	27	11

Of the respondents who reported being not interested in participating in the gig economy, over half the female respondents cited job insecurity and lack of career progression as a significant reasons. Half the female respondents also chose limited opportunities for personal growth as a reason for not wanting to participate in the gig economy.

Figure 4: Why would you not want to be a part of the gig economy?

Why would you not want to be a part of the gig economy? (%)

Gender	Job insecurity	Low salary	Lack of structure in working schedule	Lack of prestige	Lack of career progression	Limited opportunities for personal growth	Other
Male	46	39	25	24	50	47	3
Female	51	39	32	23	51	50	3
Non - Binary	50	20	40	30	30	40	10
Total	48	39	28	23	50	48	3

When asked in another manner, of those who expressed an interest in working in the gig economy for their main source of income – 59 percent of female respondents said that the salary would be a concern. Again, 56 percent reported job security to be a cause of concern. More women than men reported safety at work as a cause of concern.

It is clear that while young Indian women are open to exploring gig work as an additional source of income – they are relatively hesitant to pursue it as a career due to the perceived lack of job security, limited opportunities for career progression and personal growth.

Conclusion

The flexibility the gig economy offers may bring more women into the workforce, but it will not be empowering without addressing the structures that impact existing inequalities such as the wage gap which is already visible in the gig economy; women's disproportionate unpaid labour which could actually increase due to the flexibility that the gig economy offers; and hard-won workers' rights — which could be backtracked.

As technology has become ubiquitous in society, it is important to welcome its positive, and question its negative, outcomes. Moving forward, it must be ensured that flexible work does not lower job quality and that social protection mechanisms evolve to adapt to new forms of work. Further, in the context of informalizing workspaces, it is important to ensure the digital and physical safety of workers. Moreover, technology-enabled gig economy or platform economy can also help build equality into platforms by ensuring non-identity based valuation of digital services. This could be transformative and bring about a discrimination-free future of work.[13].

14 Supreme Court on Aadhaar: Dogged Pragmatism, Not Ideological Dogma

Sidhant Kumar

The Supreme Court finally decided on the marathon litigation that challenged the constitutional validity of the unique identification program ("Aadhaar"). The court speaking through a majority of four judges adopted a pragmatic approach to privacy while upholding the validity of Aadhaar.[1] The court restricted the scope of the program by excluding private parties from the program while creating additional safeguards.

This litigation commenced six years ago when a number of petitioners including the lead petitioner K.S. Puttaswamy approached the Supreme Court alleging that the Aadhaar program violated their fundamental rights. Initially, the government contended that privacy was not a fundamental right which was swiftly rejected by the Supreme Court in the first Aadhaar judgement ("Aadhaar I").[2] Aadhaar I declared unequivocally that privacy is a fundamental right. The Supreme Court thereafter embarked on a review on merits of the vires of the Aadhaar program ("Aadhaar II") which has culminated in the recent watershed judgment of the court.

The court framed the question before it on the assumption that efficient governance is as much an interest to be protected as is the right to privacy, as thus:

> "The Aadhaar project raises two crucial questions: First, are there competing interests between human rights and 'welfare furthering technology' in democratic societies? Can technologies which are held out to bring opportunities for growth, also violate fundamental human freedoms? Second, if the answer to the first is in the affirmative, how should the balance be struck between these competing interests?"[3]

Aadhaar II limited the scope of Aadhaar as an instrument for identification for purposes of government services and essential government functions such as taxation. The petitioners' arguments that the program principally seeks to create a surveillance state was rejected as misplaced. This decision therefore accords recognition to the government's use of personal data for the purpose of efficient use of public resources.

The court in Aadhaar I devised a three-part test that was applied in Aadhaar II to decide the legality of the Aadhaar program:

(1) a law must be the basis for the government to restrict privacy;

(2) such a law must be in furtherance of a legitimate state aim and

(3) the law enacted is a proportional means to achieve the state aim.

The objective behind the Aadhaar program and its underlying statutory framework was targeting subsidies and reducing wasteful government expenditure. This was to be achieved by devising an efficient means for verifying the identity of those who avail government subsidies and essential services. The court had already recognised the protection of revenue as a legitimate state aim which was further buttressed.

The court defines its role in balancing essential interests and competing rights:

> "As far as citizen-state relations are concerned, the Constitution was framed to balance the rights of the individual against legitimate State interests. Being transformative, it has to be interpreted to meet the needs of a changing society. As the interpreter of the Constitution, it is the duty of this Court to be vigilant against State action that threatens to upset the fine balance between the power of the state and rights of citizens and to safeguard the liberties that inhere in our citizens."[4]

The Supreme Court incorporated safeguards through Aadhaar II by restricting the government's right to disclosure of data without judicial involvement and ruling against unreasonable data retention. The court also clarified that the government must militate against the exclusionary impact of according mandatory force to the Aadhaar program by providing practicable alternate modes of proving identity. It also limits the program to the government and its essential state functions while disallowing access to private parties such as banks and telecom service providers.

The principal takeaway from these jurisprudential developments is the principle that Indian law will not adopt a dogmatic approach to privacy. Principally, the law will permit restriction of privacy in furtherance of certain essential interests such as security and revenue protection. This balancing of interests is governed by the principle of proportionality and the legitimacy of the state aim. The proportionality rules shall prevent the adoption of unduly intrusive means and guard valiantly against any arbitrariness.

The approach adopted by the court in Aadhaar II gives primacy to a principled framework for privacy. The underlying legislation was examined on the basis of privacy principles such as purpose limitation, data minimisation, data retention and security.[5] This therefore establishes the court's concerted attempt to make the privacy test an objective one. The underlying assumption of this position is that the use of data and technology is a given and the law must adapt to its unique requirements by adopting safeguards.

The judgment overall reflects a solution-oriented jurisprudential approach to privacy protection. It also rightly gives deference to the executive in formulating the use of technology in governance and public services. Finally, it sets the tone for subsequent challenges that will arise as new technologies collide with the conventional understanding of rights

15 Spectaculorum in Conversational AI

Xerxes Rudaki, Mirabai Satguru,and Cornelius Grapheus[1]

Conversation is an unequivocally singular human ability, differentiating us from all other living beings, the basis for culture and civilisation, and defining our unique level of intelligence as a species. It serves many purposes: communication, social connection, completion of complex tasks, education, entertainment. There is nothing like a heated dialogue to get us excited about a subject matter, or each other. When we talk to each other, we are leveraging contextual information and knowledge to convey emotions, arrive at an understanding of what is being said, and express our personality.

Indeed, conversation is a high-bandwidth channel where knowledge, instructions, behaviour, emotions, and many other messages are conveyed via language (written or spoken) and its structure. In our daily lives, we typically engage in spoken conversation; recent technological innovations have introduced us to the habit of instantaneous chatting. The complexity of presentation, the structure, the conduct of the interaction, and the amount of information carried by a conversation all exhibit the intelligence of the participants.

At the same time, we are surrounded by other living beings who are inarticulate in the human way, and by a stone-cold world of machines that require specialised forms of instruction and manipulation. It has therefore been the dream of human beings to interact naturally with tools that will do its bidding. Popularised in Sci-Fi literature, the concept has existed since Homer's days (for instance, Ulysses Rhapsody Σ where Vulcan is served by human-like handmaids maid of gold).

Artificial Intelligence (AI) now comes, with the promise that it will make humanity's dream come true: to have "intelligent" conversations with machines—to get information, pass instruction, acquire education, or even obtain advice in a "natural" way. The measure of success of these AI conversational systems is the Turing test, which is also a measure of intelligence: to have a conversation with a machine on a topic or task that would be indistinguishable from talking to another human. Apart from human narcissism and creativity, what fuels this quest for intelligent conversational systems is a long list of enterprise applications and strong market need for personalised conversation between businesses and their customers.

[1] The essay has been written by scientists who have successfully created the mainstream technology acquired and implemented in today's leading AI experiences by some of the world's most valuable companies. The authors have requested anonymity.

So far, the complexity and limitations of existing dialogue tools and their resulting conversational systems, have disappointed businesses and their customers. They get the job done eventually, but after great effort, high costs for development and maintenance, and relatively limited human-level interaction experience. This is because today's automated conversational systems are not actually intelligent. Designers with domain knowledge and computer expertise define and program each conversation with the scripted responses that users can expect when interacting with the automated dialogue systems. Thus, conversational systems are built based on a decision-tree logic, where the response given by the bot depends on a dialogue state defined by specific intents and keywords identified in the user's input.

IF user's input contains 'shop' or 'buy' (intent);

AND 'cellphone' or 'mobile' (product type); THEN send message with cellphone list

Typically, designers have to program three major components in order to make an automated conversational system: a) its natural language understanding part, i.e., the part that parses and analyses human language and identifies the parts that are important for the task; b) the dialogue management part, which basically identifies a state for the dialogue based on the history and the current parsed input in order to decide what to do next; and c) a response generation part, where typically the designer programs the scripted responses of the system. What this means is that the resulting systems will seem as intelligent as the effort (and patience) that was put in by the designers who created them: capturing and anticipating a large number of potential use cases and inputs, and creating appropriate and natural sounding responses. Furthermore, adapting and maintaining such rule-based dialogue systems with changing information or new information about a task is a labour-intensive and time-consuming programming job.

To mitigate these shortcomings, the next-generation dialogue systems need to be able to learn. For starters, there are two easily accessible sources of knowledge: a) examples of human-to-human interaction; and b) existing data (books, websites, manuals, databases). This is after all what business also have at hand. Companies have collected huge amounts of example conversations from the interaction between their agents and their customers over the phone or other channels (for instance, social media). Similarly, companies have abundant organised (databases, knowledge graphs, websites) or raw (documents, manuals) data that contain knowledge related to business operations and a variety of business services (booking trips) or goal-oriented tasks (maintenance, repair). However, several attempts so far for automated example-based systems have failed, and have resulted instead in unexpected or even comical results (remember the offensive Microsoft Tay and the amusing Facebook negotiating robots challenge).

The reason is that you have to be careful what data you feed the system when you train it and also what mechanism you use to produce answers.[1,2,3] Such systems will be accepted in the business world only when their responses are not free-form, but can be restricted within a set of responses acceptable by the business.

What the above highlights is a deeper truth: automated conversational systems today are missing the link with available knowledge. This connection and knowledge transfer from data is provided so far directly by human design and programming. Thus, when building an automated dialogue system, we need to recreate existing functionality from scratch, i.e., recreate our website experience in a different way, while the underlying information is the same. That means extra work for businesses to create a totally different channel to handle customer requests – which also results in lack of consistency for the user. In contrast, human agents do not have that problem. They are able to continuously acquire knowledge by observing others or from documents, assimilate new information, and appropriately organise so as to augment their capability to conduct new goal-oriented conversations. Transferring this human ability even to some extent, to our automated dialogue agents and thus learning from example dialogues and existing knowledge sources, is necessary to make progress and it is clear that the market wants it.

If we can appropriately represent knowledge about a goal-oriented task and automatically integrate it in neural network or traditionally programmed dialogue systems, we expect to have several benefits. First of all, we expect to improve performance/accuracy of response of the systems. No more dependence on how thorough and expert the system designer is; the system will learn all there is to know from available data. Ever more so, we will be able to instill some "common sense" to the systems that can carry over from application to application. The systems will be able to adapt quickly to new and changing information as well as operate and evolve in the absence of example dialogues. Still this connection of dialogue to knowledge remains elusive and is a hard problem for machines.

Takig advantage of knowledge and restricting conversational systems to the set of acceptable responses will dramatically automate their development and maintenance, but this does not mean that we do not still need to spend effort in programming them or improving their language understanding capabilities. Conversational interfaces represent a big shift in the way we are used to thinking about interaction with our "dumb" computers and "smart" phones. Conversational computing is a paradigm shift that requires designers to change their thinking, their deliverables and their design process in order to create successful bot experiences.

We expect, therefore, that major progress will be also be made in the systems and tools that allow the composition and integration of different components related to dialogue. Designers need to be able to take advantage of the strengths and facilities that different AI technologies provide either in analysing human language or in conducting dialogue learnt from different sources. Thus, over the next couple of years we will see a proliferation in the market of tools that will not only support building conversational systems from scratch, but will also allow the evolution to similar tasks, carry-over of knowledge and dialogue management, and continuous incorporation of new data.

Such conversational interfaces will grow to be the new operating system or digital mesh that will hold technologies together. Our future will be flooded with digital assistants, drones, robots, and self-driving cars. Therefore, we also need to look toward innovative ways to converse with these new devices. That means not just giving one-way instructions or queries, but conducting two-way interactions that meet our needs. That is where conversational computing comes in. We need conversation not only for form filling or step-by-step instructions, we need it because we do not know the ever changing options (e.g. tickets and dates available, or the new situations encountered) and the systems do not know our needs, preferences, or do not have our special training and wisdom at any given time, to complete a task.

Big companies are making big investments in the conversational area: Google, Apple, Amazon, Facebook, IBM, Baidu - to name just a few. And by mastering conversation, they can master the world. The next Alexa will be your home assistant[4] or your hotel concierge.[5] The next Siri or Google-Assistant[6] will be your personal assistant at the office and home. Facebook will interact with you just like one of your friends. But apart from the domination in our personal everyday lives, conversational systems will take over the business world, since they will provide faster, better, cheaper customer service. That is where companies like IBM[7] and many start-ups are making their play. There are estimates from Gartner that AI will account for 85 percent of customer relationships by 2020, and recent market analysis indicates that today 60 percent of regular customers (i.e., you and me) would prefer to talk to an automated system than a human to complete simple tasks, if it is faster and more informative. However, the majority of us (more than 70 percent) still do not trust automated systems with complex tasks or with our money. Also, most of us, the survey says, do not want to rely on automated assistants that take decisions for us. Those cases still require the human touch, somebody who understands our needs, can negotiate, is able to explain, and lead the conversation to a win-win solution.

Major strides are expected, therefore, in systems that demonstrate more human-like characteristics and that take into account more modes of interaction than just typed messages. Microsoft, for example, is working on a natural user interface (NUI)[8] that combines natural language with gestures, touch, and gazes, to help deepen the system conversations. Everything can be "felt" by sight, touch, or sound. That is the kind of multimodal conversation that will make automated conversational systems more human-like. Google recently demonstrated Duplex,[9] a concept assistant that makes appointments and reservations for you: it sounds and interacts very human-like.

AI can play a major role in this. Research is already prototyping deep learning for conversational systems that is increasingly "deeper": Instead of learning dialogue from textual dialogue examples, novel AI systems are in the works and will learn directly from spoken interactions. MILA, the research dialogue team from the University of Montreal, Facebook, Samsung, Microsoft, and Google are already working on that direction.[10,11,12,13,14] This is going to be powerful. Recall from our younger years that spoken dialogue was our major and only skill to learn, to play, and to teach others. We were able to negotiate with our parents before we were able to read and write, and we were able to describe how to play a game to our peers or coordinate to play it, before we went to school. Spoken dialogue

interaction is a rich form of intelligent communication that only becomes more sophisticated and complex over the years: it continuously incorporates what we learn from our interaction with others or from knowledge sources (like books, documents, articles, manuals).

Are we close to seeing such systems soon? Our current experience is with concatenated systems, i.e., systems that have a speech-to-text component that transcribes our speech which is then passed on to the conversational system, and the response is then read back to us. Such systems often make mistakes and get confused, resulting in negative customer experiences. One of the reasons is that they are not tightly coupled: information about what the conversational system expects is not passed back to improve the transcription system, and vice-versa an erroneous transcription is blindly passed to the conversational system. Learning directly from the spoken dialogue examples can address many of these problems and also incorporate new aspects in the automated dialogue intelligence: emotions, attitudes, expression styles, voice inflections. We will be talking to a machine that is able to understand better certain elements of our human nature and has been programmed or "trained" to respond and evoke appropriate human-like characteristics. Our interaction with such bots will not be strained and suspicious, but rather natural and assuring.

There are three kinds of companies that will likely make it big in the market of upcoming technologies: a) those that innovate in the area of AI for automatically creating dialogue systems from available data and human-to-human interactions - they are going to be the basis for the next wave of conversational products; b) those that have platforms that allow easy and fast composition of diverse dialogue-related components and their integration into applications; and c) those that use the above advanced AI algorithms and integration platforms to build evolving vertical applications that enterprises need. These three types of companies provide the three necessary layers / pillars to the AI conversational assistants market: core technology, development middleware, and application layer. Look out for the big players and for many start-ups that cover one or more of the layers. They will be the next wave of successful companies in Conversational AI.

Should the future be feared? Will AI conversational assistants heartlessly take away the allowance of the high-school kid who takes phone orders at a fast food joint in the summer? In part, these fears are well-founded. But many of these jobs are already disappearing with the advent of e-commerce, web-banking and investing, and other innovations. It has happened before with every technological progress, but what makes us more wary now is that this new wave of progress is touching on elements unique to our human nature and intelligence.

Yet, there is no need to quickly discount humans at this point. Many more new jobs will sprout from the need to curate data, create and maintain AI infrastructure, train and maintain AI systems, develop new devices and applications, and provide new expert services. Most importantly, though, the promise is that our interaction with our tools and systems will be revolutionised, in the same way that direct manipulation interfaces on our smart phones (Apple iPhone) revolutionised it 15 years ago. There is no need to fear the future. Rather, we should embrace it.

REFERENCES

01

1 Priest, George L. “The Justice Department’s Antitrust Bomb.” The Wall Street Journal. 2 June 2009.

2 Zingales, Luigi and Guy Rolnik. “A Way to Own Your Social-Media Data.” The New York Times. 30 June 2017.

3 Sunstein, Cass R. “A New View of Antitrust Law That Favors Workers.” Bloomberg Opinion. 14 May 2018.

02

1 Aus dem Moore, Jan Peter. “The Future of Jobs in the Middle East.” World Government Summit, Dubai. January 2018.

2 Spinelli Jr., Stephen. “1 Million Jobs Will Vanish by 2026. Here’s How to Prepare Workers for an Automated Future.” CNBC, Technology Section. February 2018.

3 Salha BuKattara et al. “Transforming Education in the Arab World: Breaking Barriers in the Age of Social Learning.” Arab Social Media Report, Fifth Edition, Dubai School of Government. June 2013.

4 See generally “Education in the Arab World.” Council on Arab World Relations with Latin America and the Caribbean. 2017.

5 Spinelli Jr., Stephen. “1 Million Jobs Will Vanish by 2026. Here’s How to Prepare Workers for an Automated Future.” CNBC, Technology Section. February 2018.

6 Imad El Hajj. “Future of Artificial Intelligence and Robotics: Enabling an Arab Spring” in “The Digital Arab World: Understanding and Embracing Regional Changes in the Fourth Industrial Revolution,” World Economic Forum. 2018.

7 Karim Sabbagh et al. “Understanding the Arab Digital Generation.” 2012.

03

1 The Personal Data Protection Bill, India. 2018.

2 Committee of Experts under the Chairmanship of Justice BN Srikrishna. “A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians”. 2018.

[3] Id. at 50.

[4] Committee of Experts under the Chairmanship of Justice BN Srikrishna. "White Paper of the Committee of Experts on a Data Protection Framework for India". 2017.

[5] Supra note 2, at 50.

[6] The Personal Data Protection Bill, India. 2018. Chapter X.

[7] Ibid., S 4 to 11.

[8] Ibid., S 6.

[9] Ibid., S 10.

[10] Ibid., S 8.

[11] Ibid.

[12] Ibid., S 10.

[13] Ibid., S 9

[14] Ibid.

[15] Ibid., S 12 to 17.

[16] Ibid., S 12(3).

[17] Ibid., S 13(1).

[18] Ibid., S 13(2).

[19] Ibid., S 15.

[20] Ibid., S 16.

[21] Ibid., S 17.

[22] Ibid., S 3(35).

[23] Ibid., S 19 to 21.

[24] Ibid., S 18.

[25] Ibid., S 0(2) read with s 41(3)(a).

[26] Ibid., S 45.

[27] Ibid., S 47.

[28] Supra note 2 at 121.

[29] The Personal Data Protection Bill, India. 2018. S. 27.

[30] Ibid., S 31.

[31] Ibid., S 41(3)(b).

[32] See generally Ohlin, Jens David and Larry May. "Necessity in International Law." Oxford University Press. 2016.

[33] Lawrence Hill-Cawthorne. "The Role of Necessity in International Humanitarian and Human Rights Law." Israel Law Review, 47(2): 225-251. 2014.

[34] "International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001) Report of the ILC, 53rd sess (2001) 2 Yearbook of the International Law Commission 26." UN Doc A/56/10 (2001), Art 25; and Id at 225-251. 2001.

[35] Supra note 52 at 5.

[36] UN Commission on Human Rights. "The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, E/CN.4/1985/4." 28 September 1984.

[37] Id.

[38] See the website for United Nations Human Rights Committee for a general understanding of the role of the Human Rights Committee and the process of issuing 'General Comments'.

[39] UN Human Rights Committee (HRC). CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. 8 April 1988.

[40] See generally Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37; Communication No. 488/1992, Toonan v. Australia, para. 8.3; see also communications Nos. 903/1999, para 7.3 and 1482/2006, para 10.1& 10.2. 2014.

[41] UN Human Rights Committee (HRC). General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13. 26 May 2004.

[42] Id.

[43] Report of the Office of the United Nations High Commissioner for Human Rights. "The right to privacy in the digital age, A/HRC/27.37." 2014.

[44] J Cianciardo, "The Principle of Proportionality: The Challenges of Human Rights, J. Civ. L. Stud., 3, p.177." 2010.

[45] Mattias Kumm. "Constitutional rights as principles: on the structure and domain of constitutional justice." International Journal of Constitutional Law 2: 574. 2004.

[46] Handyside v. United Kingdom, Appl. No. 5493/72 ECtHR. 7 December 1976.

[47] Article 29 Data Protection Working Party. "The application of necessity and proportionality concepts and data protection within the law enforcement sector, Opinion 01/2014." Adopted on 27 February 2014.

[48] Dudgeon v. United Kingdom, Appl. No. 7525/76 ECtHR. 22 October 1981.

[49] See also Khelil v. Switzerland, Appl No. 16188/07 ECtHR. 18 October 2011.

[50] In this case, the legitimate aim of states was "to preserve public order and decency [and] to protect the citizen from what is offensive or injurious…to provide sufficient safeguards against exploitation and corruption of others, particularly those who are especially vulnerable because they are young, weak in body or mind, inexperienced, or in a state of special physical, official or economic dependence."

[51] Supra note 67

[52] S & Marper v. United Kingdom, Appl. No. 30562/04 and 30566/04 (ECtHR 04 December 2008)

[53] Z v. Finland, Appl. No. 22009/93 (ECtHR 25 February 1997)

[54] See generally supra note 67

[55] K and T v. Finland, Appl 25702/94 (ECtHR 12 July 2001)

[56] Peter Semayne v. Richard Gresham, 77 ER 194

[57] Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, J Chandrachud's opinion, part K.

[58] Associated Provincial Picture Houses Ltd v. Wednesbury Corporation, [1947] 2 All ER 680

[59] Lee Marsons' comment on Common Law Proportionality in English Law: Are we there yet?, Administrative Law in the Common Law World Blog, comment posted on 7 September 2017.

[60] R (Daly) v. Secretary of State for Justice, [2001] UKHL 26

[61] Id.

[62] Id.

[63] Supra note 2 at 12

[64] Timothy Endicott. "Proportionality and Incommensurability in Grant Huscroft and Bradley W Miller (eds)", "Proportionality and the Rule of Law: Rights, Justification, Reasoning." CUP. 2014.

[65] Supra note 2 at 108

[66] Sahara India Real Estate v. SEBI, C.A. No. 9813 of 2011 and C.A. No. 9833 of 2011

[67] Dagenais v. Canadian Broadcasting Corp., [1994] 3 SCR 835

04

1 *Westin, Alan. "Privacy and Freedom."* New York: Athenum. *1967.*

2 Ibid., p. 324-325

3 Hardin, Garrett. "The Tragedy of the Commons", Science. 162: 1243–1248. 1968.

4 "State and Territory Regulation of Privacy: Child Witnesses in Australian Jurisdictions." ALRC. 16 August 2010.

5 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), Article 7: Regulation defining "publicly available information".

6 Greenleaf, Graham. "Private Sector Uses of 'Public Domain' Personal Data in Asia: What's Public May Still Be Private." 127 Privacy Laws & Business International Report, 13-15; UNSW Law Research Paper No. 2014-27. 1 February 2014.

7 Ibid.

8 See the website for Loi Traitements de donnØes à caractŁre personnel (LOI-WET). Refer to art. 3, § 2. 8 December 1992.

9 See the website for Hunton Privacy Blog.

10 "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." OECD. 1981.

05

1 Lewis, James A., Denise E. Zheng and William A. Carter, "The Effect of Encryption on Lawful Access to Communications and Data." CSIS. February 2017.

2 The user holds the encryption key. One example of this would be files that are encrypted and stored locally on a laptop or external hard drive are under the exclusive control of the user who encrypts the data.

3 The Chertoff Group. "The Ground Truth About Encryption." May 2015.

4 "Statement of Principles on Access to Evidence and Encryption." Department of Home Affairs, Government of Australia. August 2018.

5 The Chertoff Group. "The Ground Truth About Encryption." May 2015.

6 Bhargava, Yuthika. "Whatsapp rejects India's demand to trace origin of message." The Hindu. 23 August 2018.

7 Budish, Ryan, Herbert Burkert and Urs Gasser. "Encryption Policy and its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects." Hoover Institution. March 2018.

[8] "Assistance and Access Bill 2018." Department of Home Affairs, Australian Government. August 2018.

[9] Mann, Monique. "The devil is in the detail of government bill to enable access to communications data." The Conversation. 15 August 2018.

[10] Levine, Dan and Joseph Menn. "Exclusive: U.S. government seeks Facebook help to wiretap Messenger – sources." Reuters. 18 August 2018.

[11] Perez, Evan and Shimon Prokupecz. "Paris attacker likely used encrypted apps, officials say." CNN. 17 December 2015.

[12] Nakashima, Ellen. "FBI paid professional hackers one-time fee to crack San Bernardino iPhone." The Washington Post. 12 April 2016.

[13] Kerr, Orin and Bruce Schneier. "Encryption Workarounds." Georgetown Law Journal 989: 106. March 2017.

[14] European Digital Rights. "Encryption Workarounds: A Digital Rights Perspective." September 2017.

[15] Vandenberg, Dustin T. "Encryption Served Three Ways: Disruptiveness asthe Key to Exceptional Access." Berkeley Technology Journal Law Journal 32, no. 4. February 2018.

[16] Harold Abelson et al. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications." MIT Computer Science and Artificial Intelligence Lab. July 2015.

[17] Chertoff Group. "The Ground Truth About Encryption"

[18] Abelson et al. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications." DSpace@MIT. 2015.

[19] Duckett, Chris. "Internet Architecture Board warns Australian encryption-busting laws could fragment the internet." ZDNet. 11 September 2018.

06

[1] McKinsey Global Institute. "Digital Globalization: The New Era of Global Flows." McKinsey&Company. February 2016.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[3] California Consumer Privacy Act. 2018.

[4] Personal Data Protection Bill. 2018.

[5] European Commission. “GDPR Article 1 - Subject-Matter and Objectives.” Intersolf Consulting.

[6] “With the Regulation on the free flow of non-personal data, the European Parliament the Council and the European Commission have reached a political agreement on a new principle that abolishes data localization requirements while making sure that competent authorities can access data for the purposes of regulatory control.” European Commission. “A Framework of the Free Flow of Non-Personal Data in the EU (European Union - Fact Sheet)” EUR-Lex.

[7] “Regulation of the European Parlianemtn and of the Council on a framework for the free flow of non-personal data in the European Union.” European Commission, SWD(2017) 304 final; SWD(2017) 305 final. 2017.

[8] “Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions;” Building a European Data Economy.” European Commission, SWD(2017) 2 final; Brussels, 10.1.2017 COM(2017) 9 final, page 3. 2017.

[9] McKinsey Global Institute. “Digital Globalization: The New Era of Global Flows.” McKinsey&Company. February 2016.

[10] Rajat Kathuria et al. “Estimating the Value of New Generation Internet Based Applications in India.” ICRIER. July 2017.

[11] Singh, Jasdeep. “Cross-border data transfers in privacy-driven India.” IAPP. March 2018.

[12] “Cross-Border Data Flows: A Review of the Regulatory Enables, Blockers, and Key Sectoral Opportunities in Five Asian Economies: India, Indonesia, Japan, the Philippines, and Vietnam.” Asia Cloud Computing Association. 2018.

[13] Fan, Ziyang and Anil Gupta. “The Dangers of Digital Protectionism.” Harvard Business Review. 30 August 2018.

[14] Sharma, Prerna. “Regulating a Digital Economy: An Indian Perspective.” Brookings Institution. 25 April 2018.

07

[1] “Re-imagining India’s M&E Sector.” E&Y and FICCI. 2018.

[2] Given the lack of academic papers on the CCI in India, this article is based on available resources including research reports, together with some newspaper articles, as well as a landscape exercise of relevant segments of the CCI.

[3] We recognise that there are competing terms with overlapping remit, including the cultural and creative industries, the creative economy, the cultural sector, arts and culture, and media and entertainment, each of which carries their own definitions and legacies internationally and in India. However, discussing definitions and their relevance to the Indian context is outside the scope of this article. This article does not cover fashion, craft, design and architecture.

[4] "Highlights of Telecom Subscription Data as on 31st March." Telecoms Regulatory Authority of India. 2018.

[5] "Mobile Internet in India 2017." Internet and Mobile Association of India. 2018.

[6] "Re-imagining India's M&E Sector." E&Y and FICCI. 2018.

[7] "Indian languages defining India's internet." KPMG and Google. 2017.

[8] "IndiaTrends2018: Trends Shaping Digital India." KPMG. May 2018.

[9] Ibid.

[10] Ibid.

[11] "Re-imagining India's M&E Sector." E&Y and FICCI. 2018.

[12] See the website for "Khabar Lahariya".

[13] "IndiaTrends2018: Trends Shaping Digital India." KPMG. May 2018.

[14] "Inner Mechanics of Bigo Live, the Money Spinning App Indians Are Going Crazy about." FactorDaily. 8 August 2018.

[15] "India Year in Search 2017." Google. 2018.

[16] Tandon, Suneera. "Google Sees Gold in Indian Languages." Quartz. 29 August 2018.

[17] "Building Services for Every Indian, in Their Language." Official Google India Blog. 28 August 2018.

[18] "Indian languages defining India's internet." KPMG and Google. 2017.

[19] "IndiaTrends2018: Trends Shaping Digital India." KPMG. May 2018.

[20] "India Year in Search 2017." Google. 2018.

[21] "Rich Regional Language Content Key to Realizing Dream of Digital India." Qrius (formerly The Indian Economist). 14 September 2018.

[22] "Re-imagining India's M&E Sector." E&Y and FICCI. 2018.

[23] Sonne, L., C. Carr and M. Cutts. "Trends in Creating a Reading Culture, Report for Tata Trusts, Forthcoming." 2018.

[24] See the website for "Google Navlekha."

[25] Dalal, Mihir and Anirban Sen. "Investor Frenzy in Content Start-ups Sparks Bubble Fears." LiveMint.com. 16 August 2018.

[26] "IndiaTrends2018: Trends Shaping Digital India." KPMG. May 2018.

[27] "Re-imagining India's M&E Sector." E&Y and FICCI. 2018.

28 Ibid.

29 "The Startups behind the Ultimate Rise of Multi-channel Networks (MCN)." YourStory.com. 16 February 2015

30 "Re-imagining India's M&E Sector." E&Y and FICCI. 2018.

31 See the website for "Google Arts and Culture."

32 "Digital Music Archiving: Digital Archive of North Indian Classical Music: Phase II (special Collections) and Digital Archive of Recorded Bengali Songs." Endangered Archives Programme. 16 November 2017.

33 "National Mission on Cultural Mapping and Roadmap." Ministry of Culture, Government of India. 2018.

34 "Re-imagining India's M&E Sector." E&Y and FICCI. 2018.

08

1 See generally "Internationalised Domain Names." ICANN.org. 2018.

2 See the website for ICANN.

3 See the website for Universal Acceptance Steering Group.

4 Kende, Michael and Andrew Kloeden. "Unleashing the power of all domains: The social, cultural and economic benefits of universal acceptance." Universal Acceptance Steering Group. 11 April 2017.

09

1 Swire, Peter and Justin D. Hemmings."Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program." New York University Annual Survey of American Law 71, no. 4: 697-700. 2016.

2 The Personal Data Protection Bill. Clause 40. 2018.

3 Ibid.

4 Agarwal, Surabhi and CR Sukumar. "Telangana red-flags Data Protection Bill citing impact on startups, investments." The Economic Times. 13 September 2018.

5 Mukherjee, Arindam. "Protection for Unruly Data," Outlook India. 2 August 2018.

6 Reisman, Dillon. "Where Is Your Data, Really?: The Technical Case Against Data Localization." Lawfare Blog. 22 May 2017.

[7] This article focuses solely on legal mechanisms for accessing stored data pursuant to a Cloud Act executive agreement, and does not consider questions of real-time interception.

[8] The Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2523(b)(4)(D).

[9] Treaty between the Government of the Republic of India and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, Article 4(1).

[10] Ibid., Article 4(2)-(3).

[11] Ibid., Article 4(2)(b).

[12] Swire, Peter and Justin D. Hemmings. "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program." New York University Annual Survey of American Law 71, no. 4: 698-99. 2016.

[13] The Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. 2523(b)(4)(D)(v).

[14] India Code of Criminal Procedure, S 91.

[15] Some scholars have argued that reliance on the CrPC in spite of more specialized procedures may not be lawful. See Abraham, Sunil and Elonnai Hickok. "Government access to private-sector data in India." 2(4) International Data Privacy Law 302 no. 2(4) (2012): 304.

[16] State of Orissa vs. Debendra N. Padhi, 2 SCC 711 (2003) ("When the section refers to investigation, inquiry, trial or other proceedings, it is to be borne in mind that under the section a police officer may move the Court for summoning and production of a document as may be necessary at any of the stages mentioned in that section.")

[17] India Code of Criminal Procedure, S 93(1)a).

[18] Ibid., S 93(1)(b).

[19] Ibid., S 93(1)(c).

[20] The Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2523(b)(4)(D)(ii).

[21] Ibid., § 2523(b)(4) ("the agreement requires that, with respect to any order that is subject to the [executive] agreement") [emphasis added].

[22] India Information Technology Act, S.81.

[23] Ibid., S 69(1).

[24] India Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, R.3.

[25] India Information Technology Act, S 69(1), (3)(c) [emphasis added].

[26] The Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2523(b)(4).

27 Ibid.

28 India Code of Criminal Procedure, S 91, 93.

29 India Information Technology Act, S 81.

10

1 Press Release by PIB. “Prime Minister to Launch Digital India Week on the First July.” Ministry of Communications.

2 Buku, Mercy W. and Michael W. Meredith. “Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity.” Washington Journal of Law, Technology and Arts. 2013.

3 “Towards Financial Inclusion in China: Models, Challenges and Global Lessons.” World Bank and People’s Bank of China.

4 “Digital Payments Transactions.” Digipay.

5 “The Indian Telecom Services Performance Indicators January-March 2018.” Telecom Regulatory Authority of India. 2018.

6 Ibid.

7 Mukherjee, Sukanya. “Digital Payments To Evolve Into A $1 Tn Behemoth In India By 2023: Credit Suisse.” Inc42.

8 “Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks.” FinCoNet.

9 Lauer, Kate and Timothy Lyman. “Digital Financial Inclusion: Implications For Customers, Regulators, Supervisors, And Standard-Setting Bodies.” CGAP.

10 “Data breach incidents in India higher than global average: Thales.” The Pioneer.

11 Press Release by the Reserve Bank of India. “ATM/Debit Card Data Breach.” Reserve Bank of India.

12 Lok Sabha. “Unstarred Question No. 1872, answered by Shri Shiv Pratap Shukla.” Ministry of Finance.

13 PTI. “Bug in UPI app costs Bank of Maharashtra Rs 25 Cr in one of India’s biggest financial frauds.” Economic Times.

14 Cyber Security Incident and Important Consumer Information. “Notice Of Data Breach.” Equifax Security. 2017.

15 “Norton Cyber Security Insights Report: Global Results.” Norton by Symantec.

[16] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks." FinCoNet.

[17] Lok Sabha. "Unstarred Question no. 4521, answered by Shri P.P. Chaudhary.", Ministry of Electronics and Information Technology; Lok Sabha,."Unstarred Question no.6084, answered by KJ Alphons." Ministry of Electronics and Information Technology.

[18] Newman, Lin Hay. "The Leaked NSA Spy Tool that Hacked the World." WIRED.

[19] Newman, Lin Hay. "The Leaked NSA Spy Tool that Hacked the World." WIRED; "Customer Guidance for WannaCrypt attacks." Microsoft Technet; Press Briefing by the White House. "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea." White House.

[20] Fruhlinger, Josh. "Petya ransomware and NotPetya malware: What you need to know now." CSO.

[21] ET Bureau. "India Third Worst Hit Nation By Ransomware Wannacry; Over 40,000 Computers Affected." The Economic Times; Kumar, Ashna. "WannaCry Did Hit India And Even Central Govt Portal. So Why Did Centre Downplay The Ransomware Attack?" India Today.

[22] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks." FinCoNet. 2016.

[23] EC, "Opinion 03/2014 on Personal Data Breach Notification", European Commission.

[24] Justice KS Puttaswamy (Retd) and Anr v Union of India, (Writ Petition (Civil) No 494 of 2012). 24 August 2017.

[25] Preamble, Payment and Settlement Systems Act. 2007.

[26] Watal Committee on Digital Payments. "Medium Term Recommendations to Strengthen Digital Payments Ecosystem." Ministry of Finance. December 2016.

[27] "Cyber Security Framework In Banks." Reserve Bank of India.

[28] "Master Direction On Issuance And Operation Of Prepaid Payment Instruments." Reserve Bank of India.

[29] "Master Circular – Mobile Banking Transactions in India – Operative Guidelines for Banks." Reserve Bank of India.

[30] Department of Economic Affairs. "Press Release On The Report Of The Working Group For Setting Up Computer Emergency Response Team In The Financial Sector." Ministry of Finance.

[31] Rule 3(b)(xii), "Master Direction – You're your Customer (KYC) Direction, 2016" (Updated as on 12 July 2018). Reserve Bank of India. 2016.

[32] "Digital Payments in India Report." Akamai Technologies and Medianama.

[33] Department of Revenue. "Notification GSR 538(E)." Ministry of Finance.

[34] Justice KS Puttaswamy (Retd) and ANR v Union of India and Ors, Writ Petition (Civil) No. 494 of 2012, Order. 15 December 2017.

[35] Developed by iSPIRT, India Stack is an Aadhaar-linked set of Application Programming Interfaces (APIs) operating in "layers" that afford developers a set of tools and access to Aadhaar user data to produce curated applications and services.

[36] "United Payments Interface Procedural Guidelines." National Payments Corporation of India.

[37] "Fintech: Privacy and Identity in the New Data-Intensive Financial Sector." Privacy International.

[38] Acharya, Bhairav. "Privacy and Security Risks of Digital Payments." ORF Issue Brief 117.

[39] Watal Committee on Digital Payments. "Medium Term Recommendations to Strengthen Digital Payments Ecosystem." Ministry of Finance. December 2016.

[40] "Digital Security Risk Management For Economic And Social Prosperity." OECD.

[41] "Network and Information Security in the Finance Sector." European Union Agency for Network and Information Security.

[42] "Fundamental Elements of Cybersecurity for the Financial Sector." G7.

[43] Committee on Payments and Market Infrastructures. "Guidance on cyber resilience for financial market infrastructures." Board of International Organisation of Securities Commissions.

[44] "Network and Information Security in the Finance Sector." European Union Agency for Network and Information Security.

[45] Paul A. Grassi, et al. "Digital Identity Guidelines— Authentication and Lifecycle Management." NIST Special Publication 800-63B.

[46] "Online And Mobile Payments: Supervisory Challenges To Mitigate Security Risks." FinCoNet.

[47] Based on factors like value of transaction, and security tools adopted by the Payment Service Provider.

[48] "3-D Secure – Emvco." EMVCo.

[49] Statistics Division, Department of Economic and Social Affairs. "SDG Indicators Metadata Repository." United Nations.

[50] McCann, Niall and Lea Zoric "Harnessing digital technology for legal identity." Our Perspectives, UNDP.

[51] ITU-T Focus Group on Digital Financial Services. "Identity And Authentication." International Telecommunication Union (ITU).

[52] Ibid.

[53] Trusted Identities Group. "Overview." National Institute of Standards and Technology.

[54] Grassi, Paul A., Michael E. Garcia and James L. Fenton. "Digital Identity Guidelines." NIST Special Publication 800-63-3.

[55] "Handy-Signatur & Burgerkarte." Buergerkarte.

[56] ITU-T Focus Group on Digital Financial Services, op. cit.

[57] "Payments and Monetary and Financial Stability." European Central Bank; Bank of England.

[58] Committee on Payment and Settlement Systems. "Innovations In Retail Payments." Bank For International Settlements.

[59] European Central Bank; Bank of England, op. cit.

[60] Rule 3(ii) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules). 2011.

[61] Rule 8, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules). 2011.

[62] Kesari, Vinay. "What works and what hurts business in India's new data protection bill." FactorDaily.

[63] Committee of Experts. "White Paper of the Committee of Experts on a Data Protection Framework for India. 185." Ministry of Electronics and Information Technology.

[64] Draft Personal Data Protection Bill, S 40 and 41.

[65] Draft Personal Data Protection Bill, S 2.

[66] Defined as "data which directly or indirectly identifies the data principal." (Broad standard of identifiability adopted).

[67] Non-exhaustive list (which DPA can expand) additionally comprising passwords; health data; "official identifiers" including Aadhaar number; sex life; sexual orientation; genetic data; transgender status; intersex status; caste or tribe; religious or political affiliation or belief.

[68] Draft Personal Data Protection Bill, S 3(19).

[69] Draft Personal Data Protection Bill, S 18.

[70] Australian Law Reform Commission. "The Privacy Act: Some Important Definitions." Australian Government, 6.107, 6.180.

[71] "Special category data." The United Kingdom's Information Commissioner's Office.

[72] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians." Ministry of Electronics and Information Technology.

11

[1] Brattberg, Erik and Tim Maurer. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Carnegie Endowment for International Peace. 23 May 2018.

[2] Gleicher, Nathaniel. "What We've Found So Far." Facebook. 21 August 2018.

[3] "Report of the Attorney General's Cyber Digital Task Force." U.S. Department of Justice. 2 July 2018.

[4] Jones, Simon. "Combating Information Operations: Developing an Operating Concept." Belfer Center for Science and International Affairs, Harvard Kennedy School. June 2018.

[5] Brattberg, Erik and Tim Maurer, op. cit.

[6] Cederberg, Gabriel. "Catching Swedish Phish: How Sweden is Protecting its 2018 Elections." Belfer Center for Science and International Affairs, Harvard Kennedy School. August 2018.

[7] Ibid.

[8] Jones, Simon, op. cit.

[9] Brattberg, Erik and Tim Maurer, op. cit.

[10] Bershidsky, Leonid. "Twitter's Trolls Are Coming for Sweden's Election." Bloomberg Opinion. 30 August 2018.

[11] Stamos, Alex. "How the U.S. Has Failed to Protect the 2018 Election – and Four Ways to Protect 2020." Lawfare. 22 August 2018.

[12] Walker, Kent. "Supporting election integrity through greater advertising transparency." Google. 4 May 2018.

[13] Leathern, Rob. "Shining a Light on Ads With Political Content." Facebook. 24 May 2018.

[14] Gadde, Vijaya and Bruce Falck. "Increasing Transparency for Political Campaigning Ads on Twitter." Twitter. 24 May 2018.

[15] Brattberg, Erik and Tim Maurer, op. cit.

[16] Ibid.

[17] Nakashima, Ellen. "Justice Department plans to alert public to foreign operations targeting U.S. democracy," The Washington Post. 19 July 2018.

[18] Brattberg, Erik and Tim Maurer, op. cit.

[19] Cederberg, Gabriel, op. cit.

[20] Jones, Simon, op. cit.

[21] Benesch, Susan. "Countering Dangerous Speech: New Ideas for Genocide Prevention." United States Holocaust Memorial Museum. 12 February 2014.

12

[1] Sharma, Mihir, Terri Chapman and Samir Saran. "A New Social Contract for the Digital Age." The Observer Research Foundation; G20 Insights. 30 May 2018.

13

[1] The LFP rate used in this paper is from: Fletcher, Erin K., Rohini Pande and Charity Troyer Moore. "Women and Work in India: Descriptive Evidence and a Review of Potential Policies." CID Faculty Working Paper, no. 339:5. December 2017.

[2] According to their calculation, FLFP is calculated using the sum of all individuals employed in wage labor, own-account work, casual labor, unpaid labor, self-employment, or as an employer, plus those who are unemployed and seeking work, divided by the working-age population (15-70) not currently enrolled in school.

[3] "World Employment and Social Outlook: Trends for Women 2017"; "Danger at Sea - Working in the Fishing Sector." The World Economic Forum. June 2017.

[4] Bandare, Namita. "Why Indian Workplaces Are Losing Women." The Wire. 5 August 2017.

[5] Hunt, Abigail. "What Policymakers need to know about Women and the Gig Economy." Overseas Development Institute. 26 January 2017.

[6] Ibid.

[7] Moore, Miranda. "A study of Uber drivers found that workplace flexibility may not close the gender pay gap." The Washington Post. 9 July 2018.

[8] "Going Digital: The Future of work for Women". OECD. July 2017.

[9] "Automation, Women, and the Future of Work." Rapid Response Briefing, ESRC and DfID. July 2017.

[10] "Going Digital: The Future of work for Women." OECD. July 2017.

[11] Vidisha Mishra et al. "Young India and Work: A Survey of Youth Aspirations." The Observer Research Foundation and The World Economic Forum. 2018.

[12] Respondents could choose more than one option.

[13] Respondents could choose more than one option.

[14] Hunt, Abigail. “Back to the Future: Women’s Work and the Gig Economy.” Open Democracy. 16 May 16, 2017.

14

[1] K.S Puttaswamy v. Union of India, Writ Petition Civil 494 of 2012, September 26, 2018.

[2] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

[3] Supre Note 1 at page 12, paragraph 12.

[4] Supra Note 1 at page 13, paragraph 14.

[5] Supra Note 1 page 270, paragraph 185.

15

[1] R Chulaka Gunasekara et al. “Quantized Dialog-A general approach for conversational systems.” Computer Speech & Language. 2018.

[2] Celikyilmaz, Asli, Li Deng, and Dilek Hakkani-Tür. “Deep Learning in Spoken and Text-Based Dialog Systems.” In Deep Learning in Natural Language Processing, pp. 49-78. Springer, Singapore. 2018.

[3] Gokhan Tur et al. “Deep Learning in Conversational Language Understanding.” Deep Learning in Natural Language Processing, 23-48. Springer, Singapore. 2018.

[4] See the website for “Amazon Smart Home Devices.”

[5] Porter, Eduardo. “Hotel Workers Fret Over a New Rival: Alexa at the Front Desk.” The New York Times. 24 September 2018.

[6] “Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone.” Google AI Blog. 8 May 2018.

[7] See the website for “IBM Watson Assistant.”

[8] Pallep. “Natural User Interface, NUI - Microsoft Style Guide.” Microsoft Docs

[9] Google AI Blog, op. cit.

[10] D. Serdyuk et al. “Towards End-To-End Spoken Language Understanding.” February 2018.

[11] P. Haghani et al. “From Audio to Semantics” Approaches to End-To-End Spoken Language Understanding.” September 2018.

[12] B. Liu et al. “Dialogue Learning with Human Teaching and Feedback in End-to-End Trainable Task-Oriented Dialogue Systems.” April 2018.

[13] P. Shah et al. “Robot Navigation by Following Natural Language Directions with Deep Reinforcement Learning.” 2018.

[14] Williams, Jason D, and Lars Liden. “Demonstration of interactive teaching for end-to-end dialog control with hybrid code networks.” Proceedings of the 18th Annual SIGdial Meeting on Discourse and Dialogue. 2017.

AUTHORS

Rajeev Mantri

Rajeev Mantri is Executive Director of Navam Capital, an India-based venture capital firm. In August 2010, Rajeev co-founded Vyome Biosciences, a biopharmaceuticals company, and served as Vyome's president through the company's formative years. Rajeev is a member of the advisory board of RISE Foundation, IISER Kolkata and founding trustee of the India Enterprise Council.

Amina Khairy

Amina Khairy has been a journalist for the past 31 years. She teaches journalistic writing at the Arab Academy for Science, Technology, and Maritime Transport. She is also a media trainer and TV commentator.

Amber Sinha, Nehaa Chaudhari, Smitha Krishna Prasad

Amber Sinha is a Senior Programme Manager at the Centre for Internet and Society, India. He tweets at @ambersinha07. Nehaa Chaudhari is the Public Policy Lead at Ikigai Law. She tweets at @nehaachaudhari. Smitha Krishna Prasad is the Civil Liberties Lead at the Centre for Communication Governance, National Law University, Delhi. She tweets at @smithakprasad.

K.S. Park

K.S. Park is a professor at Korea University Law School, and co-founder of www.opennetkorea.org. Previously, he has served as Commissioner at the Korean Communication Standards Commission, and was a member of the National Media Commission He founded the Korea University Law Review and the Law Schools' Clinical Legal Education Center, and spearheaded www.internetlawclinic.org and www.transparency.or.kr.

Anushka Kaushik

Anushka Kaushik heads the cybersecurity programme at the GLOBSEC Policy Institute, a think-tank based in Bratislava, Slovakia. She's responsible for driving research efforts of the organisation in cyber policy. Prior to joining GLOBSEC, Anushka worked on data protection policies and internet governance at the International Chamber of Commerce in Paris.

Laura Sallstrom, Christopher Martin, Logan Finucan

Laura Sallstrom is Global Head of Public Policy at Access Partnership. Christopher Martin is Director of Asia Pacific. Logan Finucan is Senior Analyst of International

Public Policy. Access Partnership is the world's leading public policy firm for the tech sector. Their team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data and connectivity.

Lina Sonne

Lina Sonne is a Visiting Fellow at ORF. She works across innovation, entrepreneurship and skilling for public purpose and social impact, with a particular interest in how to strengthen ecosystems and create enabling policies. At ORF, she focuses her research on technology and society, the creative industries and the future of work. She also runs the quarterly Mumbai Tech Talk — a speaker and event series that explores technical change and urban transformation in India.

Ashwin Rangan

Ashwin Rangan is Senior Vice President Engineering and Chief Information Officer of ICANN – a not-for-profit public-benefit corporation dedicated to keeping the internet secure, stable and interoperable.

Justin Hemmings and Sreenidhi Srinivasan

Justin Hemmings is a Research Faculty Member at the Georgia Institute of Technology Scheller College of Business and a Project Attorney at Alston & Bird, where he engages in legal and policy issues and practice concerning privacy and cybersecurity. Sreenidhi Srinivasan is also Research Faculty Member at the Georgia Institute of Technology Scheller College of Business. She previously worked as Senior Resident Fellow at the Vidhi Centre for Legal Policy, a New Delhi-based think-tank, where she provided research and drafting assistance to Indian government ministries and regulatory authorities on data protection, net neutrality and areas related to the digital economy.

Sidharth Deb

Sidharth Deb is an Associate at Koan Advisory – a research-driven advisory firm, that combines legal, economic and investments expertise, and continuously engages with decision makers to deliver on client mandates in India. He works on areas relating to information technology, and the future of convergence regulations. Previously he has been associated with the Centre for Communication Governance and the Centre for Internet and Society.

Stephanie MacLellan

Stephanie MacLellan is a Senior Research Associate in the Global Security and Politics Program at the Centre for International Governance innovation, specializing in Internet governance and cybersecurity. She spent more than a decade working as an editor and reporter for newspapers such as the Toronto Star, The Hamilton Spectator and The Slovak Spectator, an English-language weekly based in Bratislava, Slovakia.

Mihir S. Sharma

Mihir S. Sharma is a Senior Fellow and Head of Economy and Growth Programme at the Observer Research Foundation. He is a trained economist and political scientist. From 2008, he edited and wrote a column for the opinion pages of The Indian Express and Business Standard, both based in New Delhi, and has won a Sriram Sanlam award for financial journalism. His book Restart: The Last Chance for the Indian Economy was published in 2015, to considerable critical acclaim; it won the Tata LitLive best Business Book of the Year and was longlisted for the Financial Times–McKinsey Business Book of the Year. He is also the India columnist for Bloomberg View.

Vidisha Mishra

Vidisha Mishra is an Associate Fellow at ORF. She currently leads ORF's work on gender and tracks the future of work, education, and skills in India. Previously, she was a Managing Global Governance (MGG) Fellow with the German Development Institute/Deutsches Institut für Entwicklungspolitik (DIE), and now she continues her association with the DIE as a consultant. Vidisha is a member of the Women20 (W20) Network and the Think20 (T20) Digital Economy Task Force of the G20. She is also a part of the UN Working Group on Youth and Gender Equality for the Commission on the Status of Women (CSW).

Sidhant Kumar

Sidhant Kumar is an advocate based in Delhi engaged in commercial and regulatory litigation. He has co-authored Privacy Law: Principles, Injunctions and Compensation, one of the first detailed books on the subject in India which was cited by the Supreme Court of India in its celebrated decision in K.S. Puttaswamy v. Union of India. Sidhant earned his Masters in Law from Stanford Law School with a specialisation in International Economic Law. Sidhant has previously worked with the noted international law firm in Singapore where he advised on corporate transactions and complex international arbitrations in Singapore, London and India.