Information and Communication Technology Dossier

A Global Perspective

CUTS International

ICTD-6: October-December 2018

As IT companies in India begin to see large deals coming their way after a few subdued years, the sector is geared up to add around 250,000 new jobs in 2019. Some of the areas experiencing fast growth are data analytics, machine learning, cloud computing and cyber-security. But living in the era of data-driven innovation, issues of national data sovereignty, and law enforcement access are prompting many governments to redesign their policy space to safeguard their economy.

The landscape is witnessing many contemporary competition issues with respect to digital markets, and has highlighted the need for major changes to privacy and consumer protection laws, alterations to merger law, and a regulator to investigate the operation of algorithms that are owned and developed by companies operating in this sphere.

This edition of the ICT Dossier covers four major stories: How Dangerous are Drones to Aircraft; Google, Facebook Face Crackdown on Market Power in Australia; India's IT Sector to Offer 250,000 Jobs in 2019; and Protesting Data Localisation Reform in Indonesia.

Like the previous edition, this ICT Dossier focuses on four verticals, namely; IPR and Competition; Innovation and Disruption; Connectivity; and Privacy and Data Ownership. Purpose of the dossier is to flag important issues for each of the four verticals, to a layperson as well as policymakers. Each story ends with several questions for the reader to contemplate and think of the way forward. This dossier may also be accessed at www.cuts-ccier.org.

CONTENTS

How Dangerous are Drones to Aircraft?

Gatwick Airport, UK suspends flights amid fears of collisions with objects that could pose serious threat. It is against the law to fly a drone higher than 120 metres or in restricted airspace, such as near an airport, as per UK laws

The rate of near misses between drones and aircraft in the UK has tripled since 2015. The UK Airprox Board (UKAB), which monitors all near misses involving commercial aircraft, said there were 92 between aircraft and drones in 2017. That was more than three times the number in 2015: 29. In 2016, there were 71 and the data is clearly tracking the growth in drone use.

Authorities around the world have explored a variety of methods to tackle rogue drones. One of the simplest involves throwing a net at the offending vehicle, either by firing it from cannon on the ground, or dropping it from a second drone. The rotors of a quadcopter rapidly get tangled in the netting and device plummets to the ground. At the other end of the spectrum, Dutch police have explored using specially trained eagles to attack drones.

There is plenty of speculation about who is behind the Gatwick drones, given the impact they have had, but the fact that the disruption was sustained for a long period points to a deliberate act. Sussex police said it was "a deliberate act to disrupt the airport", but added: "There are absolutely no indications to suggest this is terror-related."

Source: www.theguardian.com/technology/2018/dec/20/how-dangerous-are-drones-to-aircraft

Food for Thought

The global commercial drone market is expected to grow on an average of 36 percent each year to reach US$14.7bn by 2022, according to a report by market research firm Technavio published earlier in 2018. The ease of obtaining drones or unmanned aerial vehicles (UAVs) has bred a vast associated industry, and we are seeing widespread use by civilians, the military and non-state actors (NSAs). Moreover, the military and NSAs have found similar uses for drones, such as surveillance and attack purposes. And the roles that drones can perform are only limited by imagination.

Drones are becoming an increasing threat to aviation with rise in incidences between drones and airports. Threats could range from an uninformed or ignorant amateur operator breaching state rules to a terror organisation intent on inflicting mass damage and casualties. Mere spectre of a drone coupled with uncertainty, unmeasurable and unknown risks, made one of the busiest airports of Europe come to a standstill. The incident highlighted the lack of capacity of authorities to understand and contain nuisance in this pace. How will then authorities ensure both safety and security of drones or remain vigilant is question which needs an immediate answer. The regulators have been playing catch-up to ensure air safety till date, while the commercial users of drones have been rapidly adopted from sports broadcasting to land surveys.

Incidents, such as the Gatwick drone incursion continue to damage public trust in drones, as it confirms that drone technology in the wrong hands can be weaponised and cause chaos. But to see things from a positive perspective, the incidence could act as a wake-up call to policymakers across the world, and it could speed up the creation of rules and regulations to manage the sector which enables innovation to continue, allay fears and security risks.

What could be the methods which balance the interests of stakeholders involved and simultaneously mitigate the security risks? The situation has attracted knee-jerk reactions from opportunistic politicians to have strict regulations in place for ensuring security. And analysts and executives fear that such extreme measures would be unhelpful and may hinder the rapid growth of the drone industry.

Moreover, are the governments self-sufficient in designing laws or regulations for a technical space like this? Until the uncertainties are solved around drones, what should be the immediate measures, rules or regulations which do not stifle the growth of this industry? Also, fast tracking laws should be specific and cater to niche areas and not strive to regulate the entire space without holistic assessment. In that, authorities have a serious challenge at hand, to look for alternative remedies till a proper system can be identified to deal with nuisance related to drones. They may need to shift attention from how to regulate drone flights to practical ways of neutralising the threat and finding scofflaws for now.

Some of the world's largest technology companies have been keen to seize the opportunity and demonstrate the benefits to policymakers. But maybe first they need to help policymakers understand the potential risks and challenges of such technology because it looks like the next bout of drone disruption is not a matter of if, but when.

Google, Facebook Face Crackdown on Market Power in Australia

Google and Facebook Inc. face a regulatory crackdown in Australia after Australian Competition and Consumer Commission (ACCC) joined a chorus of international criticism over their use of data and the market power they wield across news and advertising.

In a preliminary report, the ACCC said a new or existing watchdog should investigate and monitor how large digital platforms rank and display adverts and news. It also expressed concern about a lack of transparency in how their key algorithms work.

"The ACCC considers that the strong market position of digital platforms, such as Google and Facebook justifies a greater level of regulatory oversight," Chairman Rod Sims said. The report contains 11 preliminary recommendations and eight areas for further analysis as the inquiry continues.

Echoing concerns in Europe, the ACCC said Google and Facebook had become the 'dominant gateways between news media businesses and audiences', leading to a loss of advertising revenue and ultimately cuts in the number of journalists who could play an

important role in 'exposing corruption and holding governments, companies, powerful individuals and institutions to account'.

The ACCC said its "preliminary view is that consumers face a potential risk of filter bubbles, or echo chambers, and less reliable news on digital platforms."

Source: www.livemint.com/Politics/4jkTgNijeTKMkESzahL4IJ/Google-Facebook-face-Australia-crackdown-over-market-power.html

Food for Thought

*On December 10, 2018, the ACCC released its preliminary report on the inquiry into the impact of search engines, social media and digital content aggregators (**digital platforms**) on competition in the Australian media and advertising services markets. The report touches base on contemporary competition issues that are currently surfacing with respect to digital markets. It also highlights the need for major changes to privacy and consumer protection laws, alterations to merger law, and a regulator to investigate the operation of algorithms that are owned and developed by the companies.*

Although the ACCC looked at digital markets generally, its prime focus was on Google and Facebook due to their 'influence, significance and size'. The Committee recognised that these platforms have considerable market power in a number of relevant markets that will only increase with time. Hence, the Commission made preliminary recommendations suggesting measures to: (a) address the market power of Google and Facebook; (b) monitor digital platforms' activities and the potential consequences of those activities for news media organisations and advertisers; (c) address regulatory imbalance by conducting a review of media regulatory frameworks; (d) assist a more effective removal of copyright infringing material; and (e) better inform consumers when dealing with digital platforms and improve their bargaining power.

While concluding the report, the ACCC outlined areas for further analysis and consideration including, but not limited to, the establishment of an ombudsman to handle complaints about digital platforms from consumers, advertisers, media companies and other business users of digital platforms, an explicit obligation to delete all user data associated with an Australian consumer once that user ceases to use the digital platform's services, and introducing a general prohibition against use of unfair trading practices.

Given the growing prominence of digital platforms across sectors, it is pertinent to understand their contemporary challenges from a regulatory as well as competition perspective. Due to their unique business models and characteristics particular to MSPs, they have garnered considerable interest amongst regulators, investors, academicians, economists and consumers. To that end, should their regulation be left at the behest of sectoral regulators or should they be governed by the competition authorities? While undertaking a competition assessment, should the authorities also take into account complex competition considerations, such as multi-homing, heavy discounting, control over data of consumers by few large players, algorithmic decision-making, common ownership, collective dominance and deep pockets?

Should the scope of enforcement through competition laws expand to cover breaches of data protection laws or privacy? Is there a need to revisit the traditional tools of competition assessment to align them with the platform economics? And lastly, to what end should platforms be allowed to disrupt the traditional markets in the name of innovation?

India's IT Sector to Offer 250,000 Jobs in 2019

After tepid job creation in 2017 and 2018, India's IT industry may be back in the market hunting for talent in 2019. As IT companies in India begin to see large deals coming their way after a few subdued years, the sector is geared up to add around 250,000 new jobs in 2019, according to HR and staffing solutions provider, TeamLease Services.

In 2017, the IT sector added over 100,000 jobs, according to NASSCOM. But the industry, one of India's top employment generators until a few years ago, laid off over 56,000 people between 2017 and 2018.

"Some of the areas wherein positive growth in hiring is expected are mathematics, architecture, and engineering-related fields," said Alka Dhingra, General Manager at TeamLease Services.

By 2020, job creation in the Indian IT sector is expected to surge to about 2 million new additions worldwide, of which around 13 percent will be in India itself, according to TeamLease. A potentially strong area of employment will be data analytics, an increasingly crucial field across industries. Other prominent roles in demand will be computer software developers, information security analysts, machine learning, mobility, cloud engineers, network analysts and cybersecurity experts.

Source: https://qz.com/india/1502573/indias-it-sector-will-have-250000-jobs-for-techies-in-2019/

Food for Thought

Amidst fears of automation taking over jobs there is a positive outlook for India's IT sector, according to estimates released by TeamLease. Following a contraction in the last few years, the sector is expected to add up to 2 million new jobs by 2020. Some of the areas experiencing fast growth are data analytics, machine learning, cloud computing and cybersecurity.

However, the IT skill gap in India continues to be a problem even as employers are now focusing on reskilling and upskilling. In 2011, NASSCOM had famously estimated that only 25 percent of technical graduates in India are considered employable. Therefore, even as there is good news for Indian IT companies, meeting the domestic demand for IT services may be a challenge.

Interestingly, experts suggest that many of the same technologies for which skills are unavailable, such as AI and blockchain, can be of great use in skill-building and on-the-job learning. AI-based adaptive programmes and blockchain-based micro-credentials are an example of this. It remains to be seen how this factors into state and private sector policies on employment and skilling.

Protesting Data Localisation Reform in Indonesia

Representatives of Indonesia's digital infrastructure operators are protesting an amendment to the country's data sovereignty laws, expressing concerns that it would be detrimental to local businesses and jeopardise data security.

The proposed reform to the Implementation of Electronic Transactions and Systems Law, which dates back to 2012, would force all so-called electronic system providers to store 'strategic' data in Indonesia, without detailing what would fall under this category.

The original text, designed to benefit 'law enforcement, protection and enforcement of national sovereignty to the data of its citizens', did not specify the type of data, merely requiring that all providers build their data centres in the country. The new proposal is hoped to attract investment in Indonesia.

Source: www.datacenterdynamics.com/news/indonesias-data-center-industry-protests-data-localization-reform/

Food for Thought

Living in the era of data-driven innovation, data has been called the new oil by many. Apart from its economic value, issues of national data sovereignty, law enforcement access, protecting domestic industries etc. have prompted many governments to implement data localisation (DL) laws. The same is true, as in the case of the most populous countries in the Asia Pacific (APAC) region — China, India and Indonesia. However, the latest draft amendment in Indonesia in this regard has made an attempt to move away from hard and strict localisation rules, and towards more cross-border flows.

Previously, there was a prevailing sense of uncertainty around the interpretation of electronic system operators that provide 'public service', who were mandated to place their data centres and/or disaster recovery centres within the boundaries of Indonesia, as per the DL laws. Since laws did not define 'public service', it had been difficult for operators to determine the applicability of the requirement on them.

The Ministry of Communications and Information Technology (MOCIT) of Indonesia's latest draft amendment to the law has removed this concept altogether. Now, electronic data has been proposed to be classified under three broad heads, namely: Strategic, High and Low Electronic Data, with only Strategic Electronic Data required being stored within the country. This has resulted in a higher threshold for attracting DL requirements for operators. Though loosely defined as 'electronic data that affects in a strategic way the sustainability of the state's administration and the state's defence and security', the move could be a welcome step in the direction of promoting a free and open global internet, if given more clarity which reduces the scope of ambiguity.

On one hand, the rules seem to be loosened up, as there is no blanket mandate of storing data locally on certain entities, on the other the country seems to have opened a box of new set of

issues/problems/uncertainties, while attempting to solve a prior issue. Earlier the blanket mandate used the terminology public service, and now its strategic data. In both situations, clarity and meaning remain elusive, as introducing strategic data concept with no clarity as to what constitutes strategic and what does not is bound to create just as much, if not more confusion. In fact segregation of data itself will be a challenge, coupled and compounded by the fact that at present only a few examples are given.

Understandably, the reason behind the diffused regulations and the confusion thereof could be because the governments hold no expertise on such subjects, but challenges like these can be tackled effectively with stakeholder consultations, and cost benefit analysis. These methodologies would help chaff out uncertainties and make rules more efficient in design as well as implementation.

Economies adjusting to rapid digital transformation may go through such shifts, as in the case of Indonesia. But policymakers need to hold wide consultations with stakeholders to reduce friction between calls for tighter controls and nationalistic agendas on one hand, and the desire for innovation and economic growth on the other. Focus should be on consumer interests emanating from cross-border data flow, as opposed to DL. And in doing so, the government must look into balancing the act, and design steps to facilitate awareness, innovation and growth.

The following issues should be looked into while undertaking such exercises:

- *A country must ensure that frequent changes in regulation will not affect the investment plans, as the need for domestic data storage and computing continues to grow*
- *The regulations designed should not be too extreme or strict, creating a situation where the baby is thrown out with the bathwater*
- *There is a need to ensure optimality within regulations, especially within the realm of disruptive and emerging technology driven businesses. Mechanisms or models of engagement should be looked at in order to minimise conflicts and increase regional and international cooperation and coordination while promoting policy goals*
- *Lastly, any limitations on cross-border data flows should address specific problems, and be least intrusive, and minimally restrictive in nature. And importance should be placed on conducting cost-benefit analysis on provisions of DL, for balancing the interests of all stakeholders, especially local industry players in this case.*

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India

Ph: 91.141.2282821 ● Fx: 91.141.2282485

cuts@cuts.org ● www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA).