Information and Communication Technology Dossier

A Global Perspective

CUTS International

ICTD-3: January-March 2018

Information and Communication Technology (ICT) and its constant evolution, like in last decade or so, remained at the centre stage of everything in the last quarter. However, one event seems to have high jacked all eyeballs: The Facebook Cambridge Analytica Scandal. Its importance is evident from the fact that the entire world is speaking about it, not just at the consumer level but in the parliaments as well.

The scandal had subjected the entire issue of data protection and privacy, as a mundane yet imperative topic of deliberation. As a positive impact, governments have taken a sigh of relief, understanding that it would have taken them ages to build capacity of consumers on big data-related concerns; a scandal would eventually cater to this imminent need -- that is a big surprise.

A lot could have been covered in this edition of the ICT Dossier, from policies for Artificial Intelligence and its possible misuse by hackers; standardising vehicle connectivity; role of cohesion policy in enhancing connectivity in Poland and Europe and many more. However, the obvious constraints have limited the dossier to four major stories: namely European Union (EU) not ruling out breaking up tech giants such as Google; US Federal Communication Commission (FCC) moving to ban Chinese made wireless gear; a self-driving Uber killing a woman in Arizona; and of course, a story on Cambridge Analytica, where Facebook is considering revamping of its privacy policy.

Like the previous edition, the ICT Dossier (Jan-Mar 2018) focusses on four verticals, namely; IPR and Competition; Innovation and Disruption; Connectivity; and Privacy and Data Ownership. The purpose of the dossier is to flag important issues for each of four verticals, to a layperson as well as policymakers. Each story ends with a few pertinent questions for the reader to contemplate and think of the way forward. This dossier may also be accessed at www.cuts-ccier.org.

Contents

EU Threatens Google with Break-up

The EU's antitrust chief has not ruled out breaking up Google over concerns about its dominance. Margrethe Vestager, the European Competition Commissioner is keeping the option open and has 'grave suspicions' as she moves forward with two separate investigations of the company.

In 2017, Vestager hit Google with a record US$2.9bn antitrust fine for favouring its own services in search results over those of competitors. The regulator is conducting two other investigations into the company's mobile platform and advertising services, which are also reportedly expected to yield massive fines.

Vestager said that Google is using its dominance in search to shut out competitors across industries. She also had to fend off accusations that she is driven by a bias against US tech giants. She stated that there is no ban on success in Europe. You get to be dominant and you get a special responsibility that you do not destroy the already weakened competition.

Source: http://thehill.com/policy/technology/380314-eu-regulator-isnt-ruling-out-breaking-up-google

Food for Thought

A few months back, there were opinions of regulating entities, such as Google (Alphabet), Amazon, Apple and Facebook, as they were becoming 'too big'. Trigger to this was the EU Competition Commission slapping a US$2.9bn antitrust fine on Google. However, the Facebook Cambridge Analytica fiasco has made these tides stronger.

These fab four tech giants are perceived to be too big and powerful, with their market cap often compared to gross domestic product (GDP) of countries. Being accused for abuse of dominance, they are also blamed for causing markets to fail. With Google controlling approx. 90 percent of search business, Amazon clocking 74 percent share in e-book market and Facebook and its subsidiaries, controlling 77 percent of mobile social traffic, many perceive that it is appropriate time to break up these tech giants, before they sit at helm of the government.

Owning to these companies dominating a number of markets, their impact on traditional businesses and competitors is often flagged. For media businesses, it is claimed that revenues for newspaper publishing and music businesses have fallen by 70 percent, courtesy tech giants. While there are allegations of this causing job and tax losses, it may also be seen as a clear case of evolution, with tech giants staying as top recruiters at tech institutions.

It may be true that these tech giants have raised the entry barriers for sectors they operate in e.g. not many companies would like to venture into web search business (a few have already tried and failed). It seems that entrepreneurship and innovation has not been severely dented as innovative businesses keep emerging, thanks to the power of ICT. However, the most successful ones have been acquired by fab four, such as Instagram and Whatsapp (Facebook), AdMob and DoubleClick (Google) and Audible, Twitch, etc. (Amazon).

Another aspect of looking at the scenario is that technology, by its basic nature seems to be monopolistic. Consumers cling on to a particular service because of their preference, making these tech giants so big. If this is the reason to break them apart, it is rather too weak. However, issues, such as biasing search results or influencing elections, hate speech and violence, do make the opposite stronger. Unlike competitors, exclusive possession of consumer data enables these tech giants to target specific consumers and offer them personalised products, while also creating new products and innovating further. Thus, the proposition for data portability may not be totally unjustified.

Considering these arguments, a few pertinent questions emerge. Is being big a major concern, or the infinite loop of exclusive growth, owing to consumer biasness which originates from exclusive possession of consumer data, impacting competition? Should the digital/tech businesses be regulated, in order to safeguard traditional businesses and stop natural evolution in its tracks or enhance consumer welfare and ensure fair markets? If yes, what should be the nature of these regulations? To prevent tech giants from growing further, is there a need to stop them from acquiring other major firms?

FCC to Slap Restrictions on Chinese-made Wireless Gear

The Federal Communications Commission (FCC) unveiled a proposal aimed at blocking certain foreign-made wireless equipment from being installed in the nation's next-generation data networks.

Under the new proposed rules, wireless carriers and other companies would not be able to use federal funds to buy networking hardware or services from 'any company that poses a national security threat to the integrity of US communications networks or the communications supply chain', according to a statement by FCC Chairman Ajit Pai.

The measure highlights growing concerns among federal officials that foreign companies which build products for international markets could write secret 'back doors' into the equipment's code that may allow others to spy on US agencies and businesses. The FCC is also seeking input on how to identify companies that pose a threat to national security and what types of devices would be covered by the proposed rule.

Source: https://www.washingtonpost.com/news/the-switch/wp/2018/03/27/the-fcc-wants-to-slap-restrictions-on-chinese-made-wireless-gear/?utm_term=.fdf9632b00a0

Food for Thought

The possible move by FCC may be seen as a major protectionist approach under the garb of protecting 'national security'. In the time where global e-trade/e-commerce and global value chain (GVC) are extensively discussed at bilateral, plurilateral and multilateral platforms, the FCC proposed stand is definitely debatable.

Against the argument given by FCC, "bar the use of money from the FCC's Universal Service Fund (USF) to purchase equipment or services from companies that pose a national security

threat to US communications networks or the communications supply chain" seems very weak, especially when all countries are contemplating on establishing rules for cross-border flow of data. Perhaps, a restriction on cross-border flow of data of national importance would have sufficed the need. However, this decision is being perceived as a political decision as a quid pro quo of the Chinese government banning some of the US entities like Facebook, to operate in their jurisdiction.

USF assists the telecom operators in providing services to remote areas. The ban will literally subject operators to use low cost hardware and networking technology from Huawei and ZTE or avail USF subsidies. This has already seen AT&T, Verizon and BestBuy, cancelling deals to carry Huawei phones in their stores. While the ban would not apply to consumers using Chinese handsets or equipment, a cascading impact on the same is quite possible. It is to note that Chinese telecom equipment, owning to low cost and easy availability have gained immense popularity across the globe in last few years and may have been instrumental in digital and financial inclusion drives across countries.

The move by FCC is much similar to the recent instances of US government banning Kaspersky, a Russian security software company, or Singapore headquartered Broadcom trying to acquire Qualcomm, where US President Trump had to step in and pulled the plug. The reason for the fallout of Broadcom-Qualcomm deal was primarily seen as the fear of US in losing out on the 5G race, where Broadcom's acquisition of Qualcomm would have allowed Chinese networking companies like Huawei and ZTE to bridge the technological gaps in US networks. Interestingly, this opens door for Nokia and Ericsson, which are not US companies either.

The US government has, in its claims, often alleged Chinese government of spying, with a fear of Chinese equipment/handsets enabling the case. However, no evidence has been revealed in public forum, to support these allegation whereas, Huawei and ZTE has publically denied these allegations. Huawei, in 2012 had also offered US to conduct a security assessment of its products, as in the case with UK, only for the US lawmakers to reject the proposal.

The entire case raises a number of questions to ponder upon, such as, is banning Chinese equipment, the only solution to safeguard national security? Would this dent the pace of digital inclusion in the country? Will this be a sector-specific approach by the US government or will this trickle down across sectors? Does this establish the inherent fear of US towards the growing prowess of China? Would US consumers support the movement, by quitting the use of Chinese handsets too?

Self-driving Uber kills Pedestrian in Arizona

An autonomous Uber car killed a woman in the street in Arizona, police said, in what appears to be the first reported fatal crash involving a self-driving vehicle and a pedestrian in the US.

Tempe police said the self-driving car was in autonomous mode at the time of the crash and that the vehicle hit a woman, who was walking outside of the crosswalk and later died at a hospital. There was a vehicle operator inside the car at the time of the crash.

Uber has been testing its self-driving cars in numerous states and temporarily suspended its vehicles in Arizona in 2017 after a crash involving one of its vehicles, a Volvo SUV. When the company first began testing its self-driving cars in California in 2016, the vehicles were caught running red lights, leading to a high-profile dispute between state regulators and the San Francisco-based Corporation.

Source: https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe

Food for Thought

After decades of research into advanced sensors, mapping, navigation, artificial intelligence, internet of things and control methods, autonomous cars are ready to hit the roads for pilot trials. However, this fatal collision could spark significant call for reforms, reflections and regulations, for and within the industry (self-regulation). Industry players are examining all available details to see what may be learned and if any course corrections are required.

Autonomous vehicle researchers, with their corporate valuations dependent on their leadership for this technology, seem to be in a race to prove their technologies in urban environment. Since urban settlements are envisaged to create maximum demand for driverless cars, their applicability to urban environment is a key quotient. Thus, there is a huge emphasis on developing successful use cases for driverless vehicles

Autonomous cars may have reached the trial phase but they might not be practical for a while, with an example evident from this accident. Earlier too, autonomous cards have been involved in unpleasant incidents, such as Google self-driving car crashing into a bus, a driver killed in Tesla car, running in self-drive mode, Uber cars jumping red lights, Volvo car knocking a group of people off their feet, etc. For a few of these incidents, federal investigators had found the technology to be at fault, but have so far resisted the urge to implement stricter rules or halt testing altogether.

Even the public has shown little sign of crusading against the technology, even after such incidents. However, analysts, while suggesting that this technology has the potential to reduce accidents and expand transportation options for disabled and elderly are stressing for more stringent safety tests. However, consideration for one aspect is completely missing: the lack of consent from citizens, who are indirectly participating in the process of testing self-driving cars.

Further, the Uber accident raises questions on the ability of safety drivers, to monitor these systems effectively, especially after long hours of testing. Even Toyota has suspended US tests of driverless cars on public roads and said it did not have a timeline for re-starting the trials. Waymo, Uber, and others had earlier urged the Congress to pass legislation that would pave way for self-driving cars in the US. The accident will most likely slow the passage of that bill.

This case highlights the mix of benefits and challenges associated with driverless cars. It also raises a number of imperative questions to be probed for answers: Is it right to test autonomous vehicles, outside of a controlled environment on public road, and posing a potential physical

threat to citizens? Who is to blame in the case of an accident involving a self-driving vehicle, i.e. the manufacturer (in case of a design fault, the software provider for buggy system software), the service centre (for inadequate service to the vehicle) or the vehicle owner (for failing to implement a software update from the manufacturer)? If such incidents keep occurring, how will the technology developers keep citizens from rallying against it? Would this leave a dent on the development of AI technology and its acceptance among consumers, across sectors?

Facebook Revamps Privacy Policy in Heels of Scandal

Facebook's new privacy policy aims to explain the data it gathers on users more clearly but does not actually change what it collects and shares. The company unveiled the revisions on April 04, 2018, as it faces one of its worst privacy scandals in history. Although Facebook says the changes are not prompted by recent events or tighter privacy rules coming from the EU, it is an opportune time. CEO Mark Zuckerberg is also set to testify before US Congress for the first time.

As Facebook evolved from a closed, Harvard-only network with no ads to a giant corporation with US$40bn in advertising revenue and huge subsidiaries, such as Instagram and WhatsApp, its privacy policy has also shifted over and over.

Almost always, critics say, the changes meant a move away from protecting user privacy toward pushing openness and more sharing. On the other hand, regulatory and user pressure has sometimes led Facebook to pull back on its data collection and use and to explain things in plainer language in contrast to dense legalese from many other internet companies.

Source: www.thehindu.com/sci-tech/technology/internet/facebook-revamps-privacy-policy-on-the-heels-of-data-breach-scandal/article23440599.ece?utm_source=email&utm_medium=Email&utm_campaign=Newsletter

Food for Thought

The Cambridge Analytica episode has triggered investigations from governments and regulators around the world. The whole fiasco is also expected to fuel demand for 'right to privacy' among consumers, including tightening of hook against 'data management' by global digital players. From the regulatory perspective, it may mark a shift from self-regulation to co-regulation or strict government regulation like EU General Data Protection Regulation (GDPR). Facebook has reportedly announced that it will apply GDPR standards to all countries (except US and Canada).

At micro level, making 'consent seeking' clear enough is most likely to happen, which will make it difficult to 'trick' consumer into providing consent. This may consequently make privacy issues less tricky to tackle. In addition, there could be more transparency on how the personal data is being used by data controllers. These may trickle down from platform's own volition or

due to regulatory mandates. However, it would be interesting to watch, if this goes further and brings in 'limitations' (e.g. for which purpose), on the collection and use of consumer data.

Further, there is likely to be enhanced restrictions on access to data from dominant players (like Facebook, Google and Amazon), for third party applications (Cambridge Analytica has allegedly accessed Facebook data though an application). A number of small businesses have prospered and grown in ranks because of access to such data. Any twist in the stance of these players towards providing access to data, might have severe implications on such small businesses. Thus, it would be interesting to see how governments would strike a balance between the prospective misuse of big data and safeguarding the growth avenues of small businesses. The Cambridge Analytica scandal does leave the world pondering over several questions.

Will there be a knee jerk regulatory intervention, which may turn out to be disproportionately restrictive than required? How the changed regulatory environment will affect the emerging digital economy? Will these trigger the change in balance of power, away from tech giants, such as Facebook and Google? How will it affect the emerging start-up ecosystem, especially in developing countries, for which access to data is crucial? Furthermore, in lieu of enhanced privacy protection, what if the so far free social platforms, become chargeable? If they do, how will it fare with consumers?

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).