# Revisiting 2020

## CCAOI Annual Newsletter

CCAOI™

Representing the ecosystem of Internet -Bharat Model

# 2020 At a Glance

Most of 2020 was overshadowed by the Covid-19 pandemic that has deeply affected nations and their economies. During the lockdown, the dependence on the Internet grew manifold and the interplay between technology (such as artificial intelligence and other emerging technologies) and health to fight the spread of the virus was very evident.

Looking back at 2020, there were several important digital policy developments at the global and national level. We are summarizing some of the main developments of 2020 (though we have shared most of these updates through our monthly newsletters). We will continue to bring you timely and neutral updates of digital policy developments from the Indian the perspective even in 2021.

Some of the key developments of 2020 have been highlighted below. For more details, please refer to the subsequent pages.

- The **growing geopolitical tensions** between US and China, security concerns related to Huawei and other Chinese companies, and at the domestic end the growing tension with China. In this regard, Tech and Trade policies dominated the discussions and continue to do so. While these frictions are expected to continue, we will need to see how things will evolve in the future.

- The **growing market power of big tech companies**, and concerns over their content policy especially towards handling misinformation and hate speech and their liabilities as intermediaries was much discussed this year.

- Issues related to **cross border data flows**, following the landmark judgement by the Court of Justice of the EU (CJEU) in the Schrems II case whereby the EU-US Privacy Shield was invalidated: While there have been some developments towards easing cross border data flow, we expect to see more developments this year.

- **Cyber Security concerns**. Not only are the frequency of cyber-attacks increasing, but they are also becoming more sophisticated and innovative, owing to the use of technology such as machine learning, artificial intelligence etc., compromising individuals, organisations and governments. The attacks in 2020 were targeted on government websites and security agencies, UN offices, companies including hotels, healthcare sector, and others. There were reports of state sponsored attacks. There was also an increase in COVID-19 themed attacks.

- Concerns related to **security of Internet of Things (IoT) devices and Artificial Intelligence (AI) ethics** continued to be debated. Various initiatives have been launched worldwide to address these issues and are expected to be discussed even in 2021.

- The growing privacy breaches, cyberattacks and use of personal data of individuals without consent, has made **data privacy and safety** a key concern for most governments and individuals. In 2020, several investigations over data privacy violations have been initiated, many countries have implemented or are in the process of implementing data protection legislations and initiatives have been taken by governments and data protection authorities to address these concerns. These discussions are expected to continue in 2021.

- **Privacy concerns** with Contract Tracing Apps and facial recognition technology

- **Challenges over the global tax structures** persisted, as there was no agreement on any clear policy

- The argument on the **status of ride hailing apps and platform workers** continued to be debated with no clear solution.

From the Indian perspective, despite the pandemic, there were several developments in the Indian Tech Policy arena in 2020. Tech geopolitics: banning of apps and making changes in FDI policy; draft data protection bill; draft non-personal data bill; liability of intermediaries especially in managing content, regulating hate speech and their growing market power; concerns related to cyber security and privacy concerns associated to contact tracing apps, were much discussed. For more details please read our section on list of month-wise developments of 2020 of Indian Tech Policy.

# Table of Contents

- Tech Geopolitics ........ 6
- Rise of Big Tech ........ 9
- Cybersecurity ........ 13
- Privacy and Data protection ........ 20
- Emerging Technologies ........ 28
- Digital Economy ........ 31
- APNIC Highlights ........ 35
- ICANN Highlights ........ 37
- Internet Society Highlights ........ 39
- India Updates ........ 41
- TRAI Updates ........ 49
- CCAOI Activities 2020 ........ 52
- Annexure ........ 58

  Reports & Articles

# The Geopolitics

2020 witnessed the growing geopolitical tensions between US and China, security concerns related to Huawei and at the domestic end the growing tension with China. In this regard, Tech and Trade policies dominated the discussions and continues to do so. While these frictions are expected to continue, we will need to see how things will evolve in the future.

## Growing US China Conflict

The US-China relations reached an all-time low this year. In May, the US accused China of adopting unfair practices to dominate the ICT industry and of creating 'security vulnerabilities for foreign countries and enterprises using Chinese vendor' and imposed trade sanctions on Chinese tech companies such as Huawei. China in turn urged US to stop "unreasonable suppression" of Huawei and warned that it will retaliate against US companies. Further, China denied the US accusation of compromising research on COVID-19.

In June, the FCC designated Chinese companies Huawei and ZTE as national security threats. In response, at the WTO, China accused the US of weakening the global tech industry's supply chain by barring US companies from using telecom equipment manufactured by companies considered to pose a national security threat.

In July, the White House issued an executive order to ban any US transactions with Bytedance and Tencent.

In August, the White House issued an executive order to ban any US transactions with Bytedance and Tencent within 45 days, subsequently through a separate executive order, it was announced that ByteDance must sell its US assets within 90 days, with Microsoft and Oracle reported to be in talks to buy parts of TikTok in this forced sale. China in turn condemned this sale and termed it as "open robbery" of Chinese technology, accused the US of damaging global trade by such sanctions and retaliated by adding several AI technologies to its export control list that experts opined could affect the discussion of the sale of TikTok in the US. TikTok on their part threatened legal action against this executive order and launched a website tiktokus.info, having collated information on the company's statements, "expert opinions" and other information "to set the matter straight".

In September, the US Department of Commerce (DoC) issued a ban on the download of WeChat, TikTok mobile applications, which was then temporarily blocked by the District Court for the District of Columbia by a preliminary injunction. It was reported that ByteDance agreed to partner with Oracle-Walmart to comply with the executive orders. China launched the

Global Initiative on data security calling other nations to put equal emphasis on development and security while adopting a balanced approach to technological progress, economic development, protection of national security and public interests.

In October, at the World Trade Organization (WTO) meeting China accused the US of violating WTO rules by banning Chinese mobile applications TikTok and WeChat. In the US, the US Cyberspace Solarium Commission released a white paper on supply chain security which elucidates to China as the principal threat.

In November, ByteDance challenged the Executive Order of divestiture in court. The US Department of Justice confirmed that it filed an appeal against a decision of a federal judge in Pennsylvania that halted the TikTok ban from coming into force on 12 November 2020 and the Committee on Foreign Investment in the US (CFIUS) granted an additional seven-7 day extension to ByteDance until 4 December 2020 to divest from TikTok.

In December, despite the deadline being passed and ByteDance not been granted an extension of the order, the negotiations with Walmart and Oracle related to divestiture of TikTok's US assets continued. The US Senators warned of national security threats from China and the FCC launched proceedings on revoking China Telecom's Authorizations. However, the Washington District Judge Carl Nichols ruled against the TikTok ban. This was the second court order against the ban.

## Concerns from other Nations

Security concerns from Chinese Tech companies, especially Huawei were much discussed in several countries across the world, including Germany, UK, Denmark, Australia, etc. The EU issued sanctions against companies in North Korea, China and Russian military intelligence services department for their stated involvement in cybercrimes. Sweden banned Huawei from participating in its 5G networks, while Finland passed a law allowing authorities to ban particular telecom network equipment.

## Mounting Indo China Tensions

In the midst of the border crisis with China, there has been growing tensions between the two countries. From the tech policy perspective, some of the developments include India making changes in the foreign direct investment rules, banning Chinese apps, and promoting Indian business.

In April, the Indian government announced changes in the foreign direct investment rules to curb "opportunistic takeovers/acquisitions" from any entity that shares a land border with India during COVID-19. It was widely seen as a move to prevent takeovers by Chinese firms during the crisis. Under the new rule, entities would be required to obtain government approval for any investment or transfer of ownership of Indian companies arising out of FDI investments.

In June 2020, 59 Chinese apps, including TikTok was banned by invoking section 69A of the IT Act. In retaliation, China blocked access to Indian newspapers and the Chinese embassy in India stated that such an action "abuses national security exceptions, and suspects of violating the WTO rules".

In July, the Indian government banned another15 Chinese apps, most of which are 'lite' or 'pro' versions of the previously banned apps.

In September, another 118 Chinese Apps were banned citing, "they are engaged in activities which are prejudicial to the sovereignty and integrity of India, defence of India, security of state and public order". It was reported that Bytedance is in talks with Softbank and Reliance Industries Limited to invest in TikTok's India operations. In retaliation, at the WTO meeting, China accused India of adopting discriminatory and restrictive trade measures by banning 234 Chinese apps and curbing foreign direct investment. India countered this by stating that China has one of the most restrictive digital economy frameworks in the world and therefore should reflect on its reluctance to open up fully to foreign trade services and transparency record.

In November, the Indian government banned another 43 Chinese mobile applications, citing security concerns taking the toll of banned apps to 267.

In the present situation, the de-escalation of the tension between the two nations seems unlikely and we will have to wait and watch how the events evolve.

# Rise of Big Tech

The **growing market power of big tech companies, and concerns over their content policy - especially towards handling misinformation and hate speech and their liabilities as intermediaries** was much discussed this year.

## Growing Power of Big Tech

To curb their market power, gatekeeping role and misuse of the role of intermediaries, there have been discussions around the world over modifying the safe harbour enjoyed by the tech companies as intermediaries, suggestions made to structurally break the companies.

The US House Judiciary Committee of the House of Representatives has published an antitrust report against the Big tech companies related to their market power, gatekeeping, abusing the role of intermediaries and in some cases suggests structural separation and line of business restrictions. Antitrust public Authorities in China released a 22-page document defining antitrust behaviour within the Chinese tech sector and proposes antitrust regulation for big tech giants. France and the Netherlands supported the proposed stricter regulations proposed by the EU to control the market position of tech companies. Britain's competition regulator the CMA informed that it had received a complaint about Google related to its market study on online platforms and digital advertising earlier this year. UK's Competition and Markets Authority has planned to limit the dominant positions of Google and Facebook.

In that context, Tech giants were called to testify before the governments. In US, the "big four" tech giants – Facebook, Google Amazon and Apple testified before the Congress virtually and CEOs of Facebook and Twitter testify before the US Senate on alleged anti-conservative bias.

In several countries, Tech companies are facing investigations. These include The European Commission opening antitrust investigations into Apple's App store and Apple Pay, the planned €2.1 billion acquisition of Fitbit by Google, filing antitrust charges against Amazon for breaching competition laws by unfairly using sellers' data to harm their businesses and the US Department of Justice (DOJ) along with 11 states filing an antitrust lawsuit against Google for breaking antitrust law by using its market power to shut out competitors. Besides, FTC ordered five major tech companies (Google, Microsoft, Amazon, Apple and Facebook) to provide detailed information on their acquisitions over the past decade as part of its antitrust investigations with a group of 165 companies writing to the European Commission seeking tougher action against Google anti-competitive practices.

In India, antitrust complaints were filed against Google over unfair promotion of Google Pay on Android Play Store in India. The Competition Commission of India (CCI) reviewed WhatsApp over allegations of abusing its dominant position by offering payment services to its app users and Google over abuse of its dominant position in its app store to promote its payments services Google Pay. The All India Vendors Association, representing more than 2000 online sellers distributing their goods through Amazon, filed an antitrust case against Amazon in India and the Ministry of Electronics and IT (MeitY) met with startup founders to understand their concerns over the 30 per cent fee Google would be charging for digital goods and services in India. Other concerns related to the tech giant were also articulated.

## Concerns related to Content Moderation and Liability of Intermediaries

With the growing trend of misinformation, hate speech and harmful content online, the debate on liability of online platforms and their content moderation policy continued to be debated.

The US Department of Justice unveiled a legislative proposal that sought to reform the safe harbour of online platforms over third party content. The Internet companies appealed to FCC to reject the proposal citing that it restricts online platform's ability to remove objectionable content.

Online companies have been facing criticism for their **content policy**. In US, Facebook faced criticism for delay in taking down content posted by right wing militia, the Thai Ministry of Digital Economy and Society filed legal action against Facebook and Twitter for not complying with takedown. In India, the Parliamentary Standing Committee on Information Technology summoned Facebook to depose before the committee for allegedly displaying hateful content on their platform. In France, the Constitutional Council found that the key provisions of the hate speech law adopted in May were unconstitutional and Facebook announced policy changes to deal with hate speech. Pakistan initially banned TikTok for allowing "indecent", and "immoral" content. However, they overturned it after TikTok's management assured that that they will block all accounts which are repeatedly involved in spreading obscenity and immorality - based on a petition seeking to remove child pornographic content from social media platforms. The Delhi High Court in India ordered social media platforms to take adequate measures to ensure that child sexual abuse content is not hosted on their platforms. The French anti discrimination organisations took Twitter to court citing that the company has taken insufficient measures to fight hate speech, after which Twitter added fact check label on the tweet of the US President. Subsequently, the organisation was accused by President Trump of stifling free speech and interfering with the US Presidential election and subsequently an Executive order on preventing online censorship was issued. In India, a petition was filed against Twitter at the Supreme Court, urging the government to create a mechanism to check content and advertisements on Twitter which allegedly spread hatred and are " against the spirit of the Union of India".

The **liability of platforms** was much debated and their safe harbour was questioned. The court of appeals in California ruled that Amazon is liable for any defective product sold by a third-party seller on its platform. The Austrian Supreme Court delivered its final judgement in the case Glawischnig-Piesczek v. Facebook Ireland Ltd, ruling Facebook to delete all defamatory statements about Austrian politician Eva Gawischnig-Pieczek globally. The US

Senate approved a legislation for combatting online child abuse and exploitation, which proposed to end the ’blanket liability protection’ for online platforms that fail to protect children from online abuse. The European Parliament committee on Internal Market and Consumer Protection voted on the committees recommendations that online platforms and marketplaces should be regulated by the Digital Services Act (DSA) package.

Some of the **initiatives taken by governments to address issues of hate speech and liability of intermediaries** include: Pakistan introducing new rules for social media companies mandating them to set up local office, localise data, remove or block content when mandated; Ethiopia passing a law curbing hate speech and disinformation online, which critics argue may stifle freedom of speech, Germany approving a hate speech bill whereby social media companies will have to report hate speech cases to the German investigator, France passing a new legislation(Avia Law) to combat online hate speech and other forms of harmful content, which has been criticised by organisation such as AccessNow and the Cyberspace Administration of China and state news agency Xinhua launching a new app to combat online misinformation.

To **curb the spread of misinformation and fake news especially during elections, some of the initiatives taken by the big tech companies** include: Facebook and Twitter taking down more than 12 disinformation networks used by political and state sponsored groups to mislead users on their platforms in the US, Saudi Arabia, Cuba, Thailand, Myanmar, Nigeria, the Philippines, and Azerbaijan, YouTube displaying warning labels on election-related videos and suspended news outlet One America News Network (OAN)for violating its policy on misinformation, Facebook banning political ads one week before US elections and updating its policies for blocking content if required to avoid regulatory risks, Twitter expanded its election related information policy and announced changes on its retweet function to tackle election misinformation in US or other civic polls, TikTok launching an elections guide to combat misinformation in US elections.

Some of the initiatives taken by **tech companies to address issues of hate speech** include- Facebook setting up a 20 member oversight board for taking ‘independent judgment’ over content policy decisions; releasing the new transparency report that elucidated information about the prevalence of hate speech on the platform and that between 0.10% to 0.11% of users violate hate speech policies, announcing changes in its policies related to hate speech in order to remove posts that denies or distorts the Holocaust; banning the QAnon conspiracy-theorist group; updating advertising policy to ban anti-vaccination ads and proposing guidelines for future regulation of online platforms for combating harmful content. TikTok appointed a seven member ‘Safety Advisory Council’ in the Asia-Pacific that comprises academics, advocates, and activists who will advise the platform on issues related to online safety, child safety, digital literacy, mental health, and human rights. Twitter announced a new conversation limit feature to restrict people from replying to tweets, of people they do not follow, or people who they have not mentioned in a tweet. A new policy has been launched to deal with deep fakes. Instagram launched a New Authenticity Measure which asks users engaging in coordinated inauthentic behavior to start verifying their identities using government and other forms of IDs and deleting comments in bulk, managing mentions and tags.

## COVID-19 related Misinformation

To curb **misinformation being spread about the COVID-19 virus**, WHO urged tech companies to take tougher action against this “infodemic”. The European Commission (EC) called on Internet platforms to provide more granular data on measures taken against COVID-19-related misinformation and in India the Ministry of Electronics and IT (MeitY) issued an advisory for social media companies to initiate awareness campaigns on their platform against such false news, take immediate action and disable and remove such content on priority and disseminate authentic information related to coronavirus. A specialist unit was set up by ministers in UK to counter disinformation about the pandemic. The EU introduced the Rapid Alert System to monitor disinformation and campaigns. The UAE announced a fine of 5500 USD if any health information related to COVID-19 was shared; WHO and Wikimedia Foundation announced that they will jointly fight against COVID-19 infodemic. The EC published the first baseline reports and third set of reports on actions taken against COVID-related misinformation by companies.

However, some of the measures taken by governments have been criticized for undermining freedom of expression. The Council of Europe (CoE) and Commissioner for Human Rights urged governments not to undermine freedom of expression and freedom of media during the pandemic. In India, industry association IAMAI stressed on adherence to the legal process for COVID-19 related Social Media takedown requests. Access Now released a guide “Fighting Misinformation and defending free expression during COVID-19: Recommendations for states” that made recommendations for governments, companies, NGOs, and individuals to protect freedom of expression and the right to impart and access information during the COVID-19 pandemic.

Platforms on their part initiated several measures to curb the misinformation being shared related to the pandemic. These include (i)a group of tech platforms (Facebook, Google, Twitter, Linkedin, Reddit) joining forces to fight against misinformation being spread related to the pandemic (ii) Instagram, Facebook and Whatsapp showing resources from WHO, Centre for Disease Control, and local health authorities, when anyone taps the hashtag related to COVID-19 (iii) Facebook removing all posts with false claims or conspiracy theories about the virus that was been flagged by global health organisations and local health authorities and notifying users who engage with COVID-19 misinformation (iv)WhatsApp limiting forwards to one person and launching a Corona Information Hub and (v) Twitter starting labelling tweets containing misleading COVID-19 information, removing tweets that can cause harm by spreading misinformation about the virus and broadening the policy on unverified claims.

While governments and online platforms are taking initiatives, looking at the magnitude and complexity of the problem, more needs to be done to address the issues related to hate speech, misinformation and content moderation online.

■■■

# Cyber Security

Cyber Security remained a much discussed topic in 2020 and is expected to be discussed equally this year. Not only are the frequency of cyber-attacks increasing, but they are also becoming more sophisticated and innovative, owing to the use of technology such as machine learning, artificial intelligence etc., which compromise individuals, organisations and governments. The attacks in 2020 were targeted on government websites and security agencies, UN offices, companies including hotels, healthcare and other sectors. There were reports of state sponsored attacks. There was also an increase in COVID-19 themed attacks mainly targeted at IoT networks.

Some of the **reports highlighting the growing incidents of cyberattack** include:

- Global Risks Report 2020 released by the World Economic Forum detailed the risks the world has experienced in the year.
- The FBI 2019 Internet Crime report highlighted that reported losses from the 467,361 complaints of suspected online crime exceeded over $3.5 billion.
- ENISA released its Cybersecurity in Railways report highlighting the cyber security challenges and need for investment in cybersecurity.
- The Office of the Australian Information Commissioner (OAIC)'s Notifiable Data Breaches (NDB) Report for January to June 2020, indicates an increase in data breaches caused by ransomware attacks and impersonation.
- Nozomi Networks published an Internet of things (IoT) security report for the first half of 2020 that reported an increase in threat to IoT networks and especially IoT botnet, ransomware, and COVID-19 themed attacks.
- The growing cyber threat was reported in Australia's ACSC Annual Cyber Threat Report July 2019 to June 2020.
- The European Union Agency for Cybersecurity's 2019 Annual Report on Trust Services Security Incidents.
- ENISA 2019 Annual Report for 2019, highlighting regulatory impact of Cybersecurity Act.
- The Microsoft Citizens on Cyberattacks Report highlighted the growing concern of nation sponsored cyberattacks.
- Kaspersky reported a growth of 350% DDoS attacks on virtual education between January to June 2020.

- India’s National Cyber Security Coordinator Lt Gen (retd) Rajesh Pant mentioned that everyday around 4 lakh malware are found and 375 cyber-attacks are witnessed.
- A report by cyber security firm Sophos indicated that 80% of Indian organizations had experienced ransomware attack
- The Kaspersky Security Network (KSN) report indicated that there had been a 37% increase in cyberattacks in the first quarter of 2020 in India as compared to fourth quarter of 2019.
- A report published by Europol, the UN Interregional Crime and Justice Research Institute, and Trend Micro highlighted the harmful uses of AI.
- The Munich Security Report 2020 released prior to the meeting touched on digital and technological security and their impact on nation states.

Some of the **reported and noteworthy cyberattacks and data breaches** include:

- Servers at the UN office of the High Commissioner of  Human Rights being hacked
- Cyber attacks on the Austrian Foreign Ministry
- Ransomware attack on Forex company Travelex
- Entire client data list of Clearwater AI being stolen
- MGM hotel databreach exposed the  personal data of 10.6 million guests,
- Ransomware attack on Chilean bank Banco Estado
- New Zealand’s Stock Exchange Market (NZX) faced distributed denial of service (DDoS) attacks
- Ritz London data breach where hackers ‘potentially compromised’ the personal data of its visitors
- European ISPS reported a mysterious wave of DDoS attacks
- Disruption of service in a few Hungarian banks and telecommunication services by a DDoS attack
- Public Health: Wales in the UK published the test results of 18 000 COVID-19 people   by mistake
- The personal data of 46 000 US veterans exposed in data breach
- Cyberattack on Indian drug maker Dr Reddy Laboratories Ltd
- Ransomware attack on Press Trust of India’s operation
- National Computer Emergency Response Team in Iran confirming that two Iranian government agencies suffered from cyberattack

- A security breach at Pegasus Technologies, a consumer finance aggregator in Uganda that plunged the telecom and banking sector in the country to a crisis
- Data breach at Manchester United
- Cyber-attack on Big Basket (a farm to home service delivery company in India) affecting 20 million users.
- Information security incident that affected multiple internal systems at Indian pharmaceutical company Lupin
- In Finland, patients' received €500 ransom call demands after Finnish psychotherapy clinic Vastaamo refused to pay €450,000
- Microsoft alleged that the attacks had been carried out on pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea, and the United States
- Portugal's Energia de Portugal was hit by a ransomware attack
- Cognizant suffered Maze Ransomware cyberattack
- Zoom passwords became available for sale in the dark web
- Iranian passwords with selfies were available for sale in the dark web
- The Twitter accounts of Joe Biden, Barack Obama, Elon Musk, Bill Gates, and others were hacked and Twitter's backend was breached and hackers tweeted a cryptocurrency scam through these accounts.
- Ransomware gang demanded $7.5 million from Telecom Argentina.
- In India, it was reported that online beauty and fashion portal Nykaa was duped of Rs 62 lakhs by cybercriminals.
- Ransomware attack on Fresenius, Europe's largest private hospital operator
- Ransomware attack on Elexon that facilitates payments on the U.K. electricity market
- Wyze breach affecting 2.4 million users
- Data breach of Indian Airline company SpiceJet affecting 1.2 million people
- MGM hotel data breach exposed the personal data of 10.6 million guests
- Canadian children's disability service unintentionally shared data of 9.000 clients
- Public Health : Wales in the UK published test results of 18000 Covid-19 persons
- Personal data of 2.4 million people were leaked by Chinese company Zhenhua Data
- Data of 1.4 Mn registered users on the job portal IIM jobs
- WhiteHat Jr data breach exposed data of 2 million users
- Personal data of 46 000 US veterans was exposed
- Miami based "value-added solutions and technology products" company Intcomex reported a data breach of 1TB users

This year, the UN First Committee (Disarmament and International Security) adopted 15 resolutions of which 2 are competing resolutions on cyberspace and international security; the UNs Open-ended working group on cybersecurity published the Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. The Council of Europe's Cybercrime Convention Committee invited comments on the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime. The EU issued a statement in support of the Council of Europe's Convention on Cybercrime. The Joint Research Centre of the European Commission published a report on cybersecurity in the EU. The National Security Agency released a UEFI Secure Boot Customization Cybersecurity Technical Report. The World Wide Web Foundation has initiated a letter asking the UN General Assembly to focus on digital security and trust.

Securing cyberspace has been a top priority for most nations. Brazil launched their cybersecurity strategy, Benin launched a new National Cybersecurity Strategy, the Australian government released their Cybersecurity Strategy 2020, the National Council of Provinces (NCOP), South Africa approved the Cybercrimes Bill. In the US, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a directive for boosting cybersecurity vulnerability reporting, the US House of Representatives passed the IoT Cybersecurity Improvement act, the US has released a National Strategy for Critical and Emerging Technologies, the US issued an Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft System, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA),under the directions of the United States National Strategy released the National Strategy to Secure 5G, the Defense Advanced Research Projects Agency (DARPA) would be investing in Encryption to Secure "Internet of Things", the Council of the European Union and the European Parliament reached a provisional political agreement on a revised regulation on cyber-surveillance technology, Australian Cyber Security Centre, DTA released new cloud security guidelines and the Australian government released a consultation paper "Protecting Critical Infrastructure and systems of National Significance". The APEC published Standards and Process-Based Approach to Enhancing Cybersecurity, Taiwan launched its financial cybersecurity plan, the Telecommunications security law was tabled in the Houses of Parliament in the UK, the Monetary Authority of Singapore released recommendations for managing cyber risks by financial institutions, Germany announced plans to create a cybersecurity agency to strengthen 'digital sovereignty', the Vietnam Ministry of Information and Communications (MIC) launched a "Review and remove malware nationwide in 2020" consultation, the CERT-In issued an advisory for companies against new ransomware, National Cybersecurity Agency of France (ANSSI) published a guide on ransomware attack, the Nigerian Communications Commission(NCC) has alerted Nigerians on the increasing incidents of financial fraud across various internet platforms and the European Commission (EC) and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy for the Digital Decade.

For securing IoT devices, the Cyber Security Agency of Singapore launched the Cybersecurity Labelling Scheme (CLS), the UK National Cyber Security Centre (NCSC) released a public recommendation urging consumers to secure their IoT and the European Union Agency for Cybersecurity (ENISA) published guidelines for securing IoT supply chain. For small and medium (SME) enterprises, the New York State Department of Financial Services announced a partnership with Global Cyber Alliance to bring a free cybersecurity toolkit for SMEs, a cyber incident response helpline was set up by UK's Scottish Business Resilience Centre (SBRC), Chilean CSIRT issued cybersecurity recommendations, the US Treasury Department issued an advisory, and Canada launched a CyberSecure certification program.

## Cybersecurity during COVID-19

There was an increase in cyberattacks during the pandemic. UNICEF reported increased vulnerability of children during the pandemic. INTERPOL's assessment of the impact of COVID-19 on cybercrime indicated a growth in the cyberattack and a shift in targets from individuals to governments and critical health infrastructure. FBI warned people of a surge in cryptocurrency-related fraud during COVID-19 and Google reported over 18 million COVID-19 related daily malware and phishing emails.

During the pandemic, there has been an increase in cyberattacks on hospitals and pharmaceutical companies manufacturing vaccine against COVID-19. Microsoft has predicted increased attacks on pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea, and the United States from Russia and North Korea.

To address the concern, various advisories were issued such as: the Indian cyber-security chief issuing a cyber-advisory for online users; the Data security Council of India (DSCI) issuing an advisory for hospitals and health care industry to fight Covid-19 related cyberattacks; the Financial Crimes Enforcement Network (FinCEN) issuing an advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic.

## Child Rights and Online Safety

With children spending more time online especially due to the pandemic, there has been a surge in child abuse online leading to concerns related to their safety on the Internet.

Several reports have indicated the rise in child abuse online. These include: UNICEF's report of increased vulnerability of children during the pandemic; Australia's ACSC Annual Cyber Threat Report July 2019 to June 2020; INTERPOL's assessment report 'Threats and Trends Child Sexual Exploitation and Abuse, COVID-19 impact' pointing to the growth of child sexual abuse online during the pandemic; a study by the International Justice Mission (IJM) revealing Philippines having the largest rate of online sexual abuse; Europol cautioning the rise in sexual abuse of children online during COVID-19; and a report by the US National Center for Missing and Exploited Children.

In India, a fourteen member adhoc committee, assessing measures to prevent sexual abuse of children online and access to online child sexual abuse material (CSAM), made forty recommendations that include permitting law enforcement agencies to break end-to-end encryption for tracing abusers, make the National Commission for Protection of Child Rights (NCPCR) the nodal agency to deal with all child related issues, appoint e-safety commissioners at state levels, install mandatory apps in all devices and filters to regulate children's access to pornography content, regulate online payments for purchasing pictures of children online and strengthen international alliances against child abuse.

Concerns were also raised on the media use of children and the role of intermediaries in protecting child rights, privacy and safety online. These concerns were highlighted in Ofcom's Children's Media Use and Attitudes report 2019 and Children's Media Lives report and the WHO report that outlined impact of online advertisement on children's health.

This has led the United States to introduce a bipartisan legislation ( EARN IT) Act to encourage tech companies to take more stringent and serious steps to protect children online. The bill proposes safe harbour for tech companies complying with the laws. However, concerns have been raised by privacy advocates and tech companies and seen as an attack on encryption.

India and Japan joined the joined the "Five Eyes" group of nations to release a joint international statement against encrypted social media platforms, urging the companies not to overlook illegal activities including the sharing of child abuse content on their platforms

The US, UK, Canada, Australia and New Zealand have released a set of eleven voluntary principles on how online tech companies can stop the spread of online child sexual abuse material (CSAM), which has been supported by coalition of tech companies that includes Facebook, Apple, Microsoft, Google and Twitter.

On their part the, The Technology Coalition, a consortium of 18 global companies that includes Facebook, Amazon, Apple, Microsoft, Google, PayPal, Snapchat, Adobe, GoDaddy, and more have announced a renewed plan to eradicate online child sexual exploitation and abuse (CSEA) through the Project Protect; Facebook announced additional tools and features in their messenger app that allows parents to have more control. However, following the company's plan to encrypt all messaging platforms, 129 child protection organisations have opposed this move.

For protecting children online, the ITU has updated and republished the guidelines on child online protection (COP). Australia released a booklet 'Online Safety for under 5s that offers advice to parents on how to keep their preschool children safe online. UK's Age Appropriate Design Code or Children's Code came into effect, the European commission passed an interim regulation related to processing of personal and other data to combat child sexual abuse, the US Senate approved a legislation that proposes to end the 'blanket liability protection' for online platforms that fail to protect children from online abuse. The French government has passed legislation that aims to regulate the earnings of online child influencers and creators.

## Cross border Data Flow

**Cross border data flows** was much discussed following the landmark judgement by the Court of Justice of the EU (CJEU) in the case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (also known as the 'Schrems II case') whereby the EU-US Privacy Shield was invalidated while Standard Contractual Clauses (SCC) was still valid.Hailed in Europe. The US expressed deep disappointment with this judgement. Within Europe, the Swiss Data Protection Authority (FDPIC) announced that it did not consider the Swiss-U.S. Privacy Shield to be adequate any longer for the purposes of transfers of personal data between the two nations while the Council of Europe (CoE) called for greater oversight on intelligence services' over international data transfers and Oracle announced to stop offering third-party data targeting services across the EU, Switzerland, the UK.

The U.S. government released a white paper on privacy safeguards relevant to standard contractual clauses (SCCs) and other EU legal bases for EU-U.S. data transfers after Schrems II and called for clarity on data transfer between EU-US.

The US Department of Commerce and the European Commission initiated discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to address the current impasse.

For easing the deadlock, The European Commission published a draft implementing decision on standard contractual clauses (SCCs) for the transfer of personal data to third countries pursuant to the EU General Data Protection Regulation, along with a draft set of new SCCs.

We expect to see more development to ease the cross border data flow this year.

# Privacy and Data Protection

The growing privacy breaches, cyberattacks and use of personal data of individuals without consent, has made data privacy and safety a key concern for most governments and individuals.

Concerns over privacy of data were raised in several countries including UN organisations who issued a joint statement highlighting the importance of data protection and privacy in the response to COVID-19. The German data protection authority urged federal agencies not to use WhatsApp; Supreme Court in India issued notice in suit to ban Zoom due to privacy concerns; the Columbian data protection authority gave TikTok ten more days to improve data protection standards before taking punitive action that includes fines of up to US$460 000 for failure to comply; Belgian DPA and Facebook had a face-off at CJEU over GDPR's one-stop-shop mechanism.

In terms of data privacy **violations and investigations** initiated, the Australian Information Commissioner filed a case against Facebook over noncompliance to the Australian Privacy Act 1988, the Attorney General of Arizona filed a law suit against Google for illegally tracking location of Android smartphone users, the Dutch Data Protection Authority initiated investigation into child privacy practices of TikTok, Germany's Federal Supreme Court ordered Facebook to stop harvesting user data across its platform, and Google faced a US$5 billion lawsuit for breaching privacy for illegally tracking users in opting for private mode. The OAIC and the UK's Information Commissioner's Office (ICO) launched a joint investigation into Clearview AI's personal information handling practices, Facebook mistakenly revealed third-party app data-sharing issue, Privacy International (PI) filed a complaint against the French health website Doctissimo over data protection issues, Amazon, Google, and Microsoft were sued over alleged violations of Illinois' Biometric Information Privacy Act that prohibit the use of personal biometric data without the data subject's permission, Walmart faced lawsuit under California's privacy law and for failing to protect customer data from an alleged hack. New Zealand's (NZ) Privacy Commissioner launched an inquiry into COVID-19 patient privacy breach, French regulator CNIL launched an investigation against TikTok over GDPR breach, Instagram was accused of collecting biometric data of users without consent, Dutch privacy group, the Privacy Collective along with support from other interest groups, filed an official class action suit against Salesforce and Oracle for GDPR violations, and the Irish Data Protection Commission (DPC) launched two investigations into Facebook after privacy concerns were raised about its handling of children's personal data on Instagram. The Supreme Court of UK ruled that employers are not liable for employee data leaks, the Court of Justice of the European Union (CJEU) ruled bulk data collection by EU national agencies as unlawful, the French court ruled that the health data of French citizens can be hosted on US companies' cloud, a US judge ruled against Twitter's bid to reveal government surveillance requests, and a Washington Attorney General sued Facebook over political ads. Google was fined approximately 7 million euro by the Swedish data protection authority (DPA) in a right to be forgotten case. In France, Google lost appeal against the €50 million fine ($56 million USD) imposed in 2019 by CNIL.

Additionally, Noyb, a European privacy group, filed 101 complaints in all 30 EU and European Economic Area (EEA) member states against 101 European companies, for continuing to use Google Analytics or Facebook Connect one month after the EU-U.S. Privacy Shield was nullified by the Court of Justice of the European Union (CJEU), US based digital rights non-profit; Electronic Frontier Foundation (EFF) filed comments in opposition to the new plans of the US Department of Health and Human Services (HHS) surveillance of COVID-19 patients, and Privacy International (PI) and 13 other civil societies from Europe and Africa urged for reforms to EU aid and co-operation programmes to ensure they promote privacy protections and human rights in third countries.

Following Europe, **several countries have implemented or are in the process of implementing data protection legislations**. In India the Data Protection Bill is being discussed by the joint Parliamentary committee. The new Privacy Act came into force in New Zealand, the European Union launched the European Strategy for Data, Republic of Northern Macedonia adopted the Law on Personal Data Protection, Dubai enacted the new Dubai International Financial Centre (DIFC) Data Protection Law, South Africa's comprehensive privacy law- Protection of Personal Information Act ('POPIA') came into effect, the Egyptian president endorsed law No. 151 of 2020 on the protection of personal data protection, Canada introduced a new data protection legislation, the Parliament of Singapore adopted proposed amendments to the Personal Data Protection Act (PDPA), Malta ratified the amending Protocol to the Convention for the Protection of Individuals with regard to the Processing of Personal Data (CETS 223) to the Council of Europe (CoE), the European Data Protection Board (EDPB) adopted a statement on the ePrivacy regulations, affirming to complement the GDPR regulations and providing additional strong guarantees for confidentiality and protection for all types of electronic communication and adopted recommendations on measures that supplement transfer tools to ensure compliance with EU standards of personal data protection, as well as recommendations on the European Essential Guarantees for surveillance measures; the EDPB adopted its Strategy 2021-2023,

In terms of **initiatives taken by governments and data protection authorities** around the world, Economic Commission for Latin America and the Caribbean (ECLAC) commissioned a study to review Caribbean data protection frameworks, the data protection authority (DPA) of the German state Baden-Württemberg released guidance on data transfers following the ruling in 'Schrems II'case, the European Data Protection Board (EDPB) published its opinion on the draft accreditation requirements for the code of conduct monitoring bodies submitted by the Dutch data protection authority (DPA), the Ontario government in Canada announced the launch of consultations to improve the province's privacy protection laws, the Chinese legislature passed the draft legislation on data protection for review and accepted public comments on draft data protection law, the European Data Protection Board (EDPB) adopted guidelines on the concept of relevant and reasoned objection, the Swedish data protection authority (DPA) released guidance on the processing of employees' personal data by private or public entities. The New Zealand Office of the Privacy Commissioner announced the launch of a new tool for organisations to report privacy breaches, the Danish data protection authority published guidelines on data processing for website visitors, the European Data Protection Board released guidelines on consent under the GDPR, the European Commission published a draft implementing decision on standard contractual clauses (SCCs) for the transfer of personal data to third countries pursuant to the EU General Data Protection Regulation, along with a draft set of new SCCs, the US Senator published a bill on Data Protection Act aimed at establishing a new independent data protection agency in the USA, the Belgian data protection authority (DPA) released data protection toolbox for data controllers and processors; Spanish data protection authority (DPA) released a paper on data protection in public administration; the Office of the Privacy Commissioner of Canada (OPC) published a set of recommendations to reform the country's Personal Information Protection and Electronic Documents Act (PIPEDA), the European Commission solicited feedback on GDPR's efficiency, the Belgian data protection authority (DPA) released data protection toolbox for data controllers and processors, Spanish data protection authority (DPA) released a paper on data protection in public administration, and the Office of the Privacy Commissioner of Canada (OPC) published a set of recommendations to reform the country's Personal Information Protection and Electronic Documents Act (PIPEDA). The European Commission published its proposed draft of the EU Data Governance Act (DGA), which outlines how digital services should handle data in the future and is part of the 2020 European Strategy for Data and European Commission decided to conduct a two year evaluation of the GDPR.

In order to protect **privacy and rights of children online**, the Committee of Convention 108, at the Council of Europe, adopted the Guidelines on Children's Data Protection in an Education Setting, during the 40th plenary meeting. The European Commission (EC) suggested suspending part of a new privacy directive that came into force at the end of December for a period of five years, UNICEF released a six-point plan and data and advocacy brief, 'Averting a lost COVID Generation', to protect children during the pandemic, the French government passed a legislation that aims to regulate the earnings of online child influencers and creators, China amended its law on the Protection of Minors by adding 60 new articles and updating some of the previous articles including a new chapter to deal with online child protection and the rights of children online.

Further in 2020, several tech companies announced a plan to stop complying with the Hong Kong government's requests for user data, Microsoft announced new steps to support data protection in EU, WhatsApp sued the Israeli company NSO for hacking attempts on 1400 users and Facebook launched legal action against two websites for harvesting personal information of users using unauthorised automation software.

## Privacy concerns with Contract Tracing Apps

In a bid to contain and reduce infection of COVID-19, most countries (Australia, South Korea, Singapore, USA, UAE, Phillipines, India, Italy, Turkey, Germany) have adopted contact tracing apps. Features of such apps include tracking people who are under quarantine or infected; and facilitating people to know if they are near any infected person. While countries like Australia, India recommend using the app, in some others like Singapore it is being made mandatory . Various companies such as Apple and Google have also developed interoperable contact tracing COVID-19 tools.

While many agree that such apps can help in tracking and trying to contain the spread of the virus, concerns have been raised about surveillance, data privacy and security of the data being collected; including how and where it is being stored, along with human rights implications (personal data of 200 users were leaked from a Dutch contact tracing app, and Israeli court declared the need for legislation for tracking COVID-19 patients digitally. European Digital Rights (EDRi) network of organizations called for a ban on biometric mass surveillance apps; the Conseil d'Etat, France's highest administrative court banned police from using drones to track people violating social-distancing rules during COVID-19. Nearly 300 academics issued a joint letter, expressing their support for the deployment of a privacy-friendly contact tracing app. Amnesty International raised concerns over the contract tracing app being used in Kuwait and Bahrain; the Electronic Frontier Foundation (EFF) called on the California Governor and state lawmakers to ensure privacy protection in all COVID-19 contact-tracing apps and urged universities that have launched or plan to launch COVID-19 tracking technologies to make them entirely voluntary for students and disclose details about data collection practices). In some places, the apps were stopped (Norway stopped its COVID-19 contact tracing app over privacy concerns)

Some guidelines issued for protecting privacy of healthcare data being stored and processed include those from European Data Protection Supervisor, European Data Protection Board, and Electronic Frontier Foundation. The EU developed an EU toolbox for interoperability of contact-tracing and warning apps within the EU, the EC announced the adoption of an Implementing Decision to support the setting up of a voluntary gateway service; among companies. Google, Facebook have announced that any location data sharing with health authorities or tools being developed to track COVID-19, should adhere to privacy norms.

## Concerns related to Facial Recognition Technology (FRT)

While there has been an increase in the adoption of surveillance technology such as Facial Recognition Technology (FRT) across the globe (Canadian police experimenting with FRT; London police using live FRT, FRT being used in schools in New York district; AI and temperature scanners are being used in China to screen people for symptoms of the coronavirus. India plans to deploy FRT by the Vadodara City Police and Railways; the London police plans to deploy FRT), concerns related to privacy and human rights over the use of such technologies continue. The Members of the European Parliament (MEPs) from the Civil Liberties Committee expressed concern over the plan to establish a common facial-recognition database for police authorities. In a report, the Human Rights Watch (HRW) has expressed concerns over the expansion of facial recognition systems in Russia and CNIL, in which the Commissioner remarked that the FRT violates GDPR). In 2020, there have been instances when courts have ruled against the use of FRT (a French court), and the use of FRT has been halted by the states. (In the US, Senators have proposed to temporarily restrict the use of FRT by government without a warrant, Portland in US introduced two ordinance against FRT (first, second); EU contemplating a temporarily ban on the use of FRT in public places; Vermont in US approved a bill that placed moratorium on police using facial recognition technology). With regard to companies, IBM announced they would not offer general purpose FRT, Amazon launched a one-year halt on police use of its FRT system, Microsoft announced it will not sell FRT to police until human-rights-based legislations are adopted and in a letter amd IBM called the US government to limit facial recognition exports)

Some discussions are underway on how to ensure human rights perspectives when such technologies are deployed. The Global Privacy Assembly adopted a resolution on facial recognition technology and CNIL released guidance for the use of facial recognition technologies in airports.

Policy discussions this year will continue to discuss how to balance the privacy and rights of people when such technologies are deployed.

## Reported Fines for Data Breaches and Privacy Violations

Most of the fines reported in 2020 were related to data breaches, privacy violations, sharing of user data without proper consent, etc. Listed below are some of the reported fines of 2020.

| Agency fined | Fined by | Reason | Amount |
|---|---|---|---|
| Facebook | Brazil | Improper sharing of user data | 1.6 million USD |
| Facebook | Illinois | Illegally collecting and storing facial recognition data | 550 million USD |
| Dixons Carphone | Information Commissioner's Office (ICO), UK | Data of 14 million people compromised | 500,000 Pound |
| Cathay Pacific | Information Commissioner's Office (ICO), UK | Failing to protect customers personal data | 500,000 Pound |
| Facebook | Germany | Failing to appoint a DPO | 55,500USD |
| XferaMóviles, Mobile company | Spain | Violating GDPR | 60,000 euros |
| Google | Swedish Data Protection Agency | Right to forgotten case | 7 million euro |
| Apple | French competition Authority | Over restrictions on contracts with wholesalers | 1.1 billion euro |
| Tusla | Ireland DPA | Privacy breach | 75,000 euro |
| Facebook | Canada fined Facebook | False privacy claims | 6.5 million USD |
| Google | France | GDPR breach | 56 million USD |
| Bank of Ireland | Ireland | Regulatory breaches cyber frauds | 1.7 million euro |
| WINDTRE, Italian telecom operator | Italy -Italian DPA | GDPR violations | 16.7 million euro |
| Google | Belgium DPA | Right to forgotten case | 600,000 euro |
| Spartoo, French retailer | CNIL France | GDPR violations | 250,000 euro |
| Capital One | US Regulators | Data breach | 80 million USD |
| Health Engine | Australia | Sharing patient data without consent | 2.9 million AUD |

| Agency fined | Fined by | Reason | Amount |
|---|---|---|---|
| China Merchants Bank Co., Ltd. Credit Card Center | Shanghai Supervision Bureau of China Banking and Insurance Regulatory Commission | Failing to protect personal data of their consumers | 120000 euro |
| Norwegian Public Roads Administration | Datatilsynet, Norway | GDPR violations | 40000 euro |
| Facebook | USA | Biometric Information Privacy Act (BIPA) lawsuit | 650 million USD |
| H&M | Data Protection Authority of Hamburg(HmbBfDI) | GDPR breach and Illegal surveillance | 35.2 million euro |
| Hospital and private company | Italian DPA | Issued two fines | 140,000 euro |
| City of Vilnius | Lithuania data protection authority (DPA) | Improperly processing data | 15,000 euro |
| SC Marsorom, | Romanian DPA | GDPR violation | 3000 euro |
| Globus Score | Romanian DPA | GDPR violation | 2000 euro |
| Facebook | South Korean agency for protecting personal information | Providing users' personal information to other operators without consent | 6.06 million USD |
| Ticketmaster UK | Information Commissioner's Office (ICO), UK | Failing to keep its customers' personal data secure following a cyber-attack on the Ticketmaster website in 2018 | 1.25 million pounds |
| Carrefour Banque | French data protection authority CNIL | GDPR and electronic communications code breaches | 800,000 euro |
| Tusla Child and Family Agency | Irish Data Protection Commission's (DPC) | Sharing data of minor without consent | 75,000 euro |
| Google | Turkish Competition Board has fined Google | Abusing its dominant market position | 26 million USD |
| PayPal | Financial Intelligence Unit, India | Violating anti-money laundering process | INR 96,00,000 |
| Google | French data protection authority CNIL | Cookies management on its search engines | 121 million USD |

| Agency fined | Fined by | Reason | Amount |
|---|---|---|---|
| Amazon | French data protection authority CNIL | Placing cookies which are tracking devices on people’s computers without their consent | 35 million euro |
| Posti Oy | Finnish office of the data protection ombudsman | GDPR breach | 100,000 euro |
| Kymen Vesi | Finnish office of the data protection ombudsman | GDPR breach | 16,000 euro |
| A company (name withheld) | Finnish office of the data protection ombudsman | GDPR breach | 12,500 euro |
| Facebook | US | Settlement to Moderators who developed Post Traumatic  Stress Disorder (PTSD) | 52 million USD |
| Norwegian Public Roads Administration | Norwegian data protection authority, Datatilsynet | GDPR violations | 40,000 euro |
| Twitter | Irish DPA | GDPR violations | 450,000 Euro |
| Twitter | Russian Court | Breaching Data Localisation rules | 4 million Rubles |
| Facebook | Russian Court | Breaching Data Localisation rules | 4 million Rubles |

# Emerging Technologies

In terms of emerging technologies, concerns related to security of Internet of Things (IoT) devices and Artificial Intelligence (AI) ethics continued to be debated. Various initiatives have been initiated worldwide to address these issues and are expected to be discussed even in 2021.

## Artificial Intelligence

The International Research Development Centre released the 2020 edition of the Government Artificial Intelligence (AI) Readiness Index that indicates that the  top five places in the index are occupied by US, UK, Finland, Germany, and Sweden, reflecting the fact that North America and Western Europe are the highest scoring regions overall in terms of AI readiness and global south countries are lagging behind. China has been ranked 19th., while India is at 40th position among 172 countries listed.

In 2020, the OECD launched an AI Policy Observatory; the Global Partnership on AI was launched to guide 'the responsible development and use of AI', where India is a member, while announcing the Roadmap for Digital Cooperation.  The UN Secretary-General shared plans to establish a multi-stakeholder advisory board on global AI co-operation.

Ethical issues related to AI were much discussed. The G20 Digital Ministers adopted a declaration to promote a human-centered approach to artificial intelligence (AI) and support for the G20 AI Principles.  The US Department of Defense (DoD) adopted ethical principles for the use of AI.  The Committee on legal affairs in the European Parliament approved and adopted three reports on artificial intelligence (AI) recommending - a framework of ethical aspects of AI, robotics, and related technologies, a civil liability regime for AI and intellectual property rights for the development of AI technologies.  The Global Privacy Assembly adopted a resolution on accountability in the development and use of AI, the Presidency of the Council of the EU issued a set of conclusions on the charter of fundamental rights in the context of artificial intelligence (AI) and digital change, highlighting that the design, development, deployment, and use of AI must fully respect fundamental rights and existing legal rules.  The standing committee of the parliamentary assembly of the council of Europe adopted a resolution and a recommendation calling for adopting a democratic governance of AI.  The US Intelligence Community (IC) released a set of Principles of AI Ethics and an AI Ethics Framework to guide the IC's ethical development and use of AI.

Besides, the European parliament announced first set of EU rules for AI, Hungary drafted AI strategy, Brazil announced the creation of a national innovation network focused on AI, India, launched the national artificial intelligence portal (www.ai.gov.in)for all AI related development, Microsoft announced building an AI supercomputer, the US army announced plans to study how soldiers interact with artificial intelligence (AI), Australia created new tools to address Algorithmic biases in AI.

The Legal Affairs Committee in the European Parliament initiated discussions on three draft reports related to AI -intellectual property rights for the development of AI technologies, a framework of ethical aspects of AI, robotics, and related technologies and potential civil liability regime for AI.

The US (White House) published 10 principles for AI regulation; European Commission published a White Paper on AI, the UK Information Commissioner's Office has published a Guidance on AI and data protection, the White House issued a memorandum providing guidance to federal agencies to consider when developing regulatory approaches to AI applications.

The Partnership on AI initiated "Closing Gaps in Responsible AI" project; IEEE Standards Associations announced three new initiatives in the field of data and artificial intelligence (AI)- the IEEE Global AI Systems (AIS) Well-being Initiative, IEEE Applied AIS Risk and Impact Framework Initiative and IEEE Trusted Data & AIS Playbook for Finance Initiative.

## Internet of Things (IoT)

The advantages of IoT was highlighted in a white paper on How Digital Transformation and IoT can contribute to the UN Sustainable Development Goals published by the IoT Alliance Australia (IoTAA) and the Industrial Internet Consortium (IIC) and a report released by the Australian Council of Learned Academies (ACOLA) and the Australian Research Council (ARC) highlighting the advantages of IoT for Australia.

A study conducted by University of Texas points to the role of the private sector in IoT governance, while a study by University of Liverpool revealed privacy threats from IoT devices and biometric.

In terms of standardization, in 2020, ISO along with IEC has launched three IoT standards - ISO/IEC 21823-2,ISO/IEC TR 30164andISO/IEC TR 30166, the ETSI Technical Committee on Cybersecurity (TC CYBER) published a new standard for IoT cybersecurity -ETSI EN 303 645 and the Web of Things Working Group of W3C (World Wide Web Consortium) issued two new recommendations for web integration across Internet of things (IoT) platforms Web of Things (WoT) Architecture, and applications WoT Description.

The US Senate passed the Developing and Growing the Internet of Things (DIGIT) Act, China announced its mobile Internet of Things (IoT) network policy and launched two communication satellites for its IoT project; the US National Institute of Standards and Technology (NIST) published the second public draft of recommendations for IoT Device Manufacturers. The US released a National Strategy for Critical and Emerging Technologies and the Cyber Security Agency of Singapore announced the launch of the IoT Cybersecurity Labeling Scheme (CLS), the US General Accountability Office published a report about federal agencies' use of IoT devices and technologies and the Australian Cyber Security Centre released an IoT guide for manufacturers 'Code of Practice: Securing the Internet of Things for Consumers'.

Security of IoT devices was much discussed. The UK government published security requirements for IoT devices, the US National Institute of Standards and Technology (NIST) published the NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers and called for public feedback for federal profile of IoT devices cybersecurity capability core as established in NISTIR 8259A. The US House of Representatives passed the IoT Cybersecurity Improvement Act, the Spanish National Cybersecurity Institute (INCIBE) published an Internet of things (IoT) security guide for companies, European Union Agency for Cybersecurity (ENISA) published guidelines for securing IoT supply chain; the Business Software Alliance published The BSA Policy Principles for Building Trust in Internet of things (IoT) devices that lays 12 principles governments should take into account when developing IoT security policies, the European Union Agency for Cybersecurity (ENISA) published guidelines for securing IoT supply chain and the US National Institute of Standards and Technology (NIST)published draft reports NISTIR 8235, Security Guidance for First Responder Mobile and Wearable Devices and Securing Small-Business and Home Internet of Things (IoT) Devices. Mitigating Network-Based attacks Using Manufacturer Usage Description (MUD)for public comments.

## Others

- Besides, the European Commission published a report on Ethics of Connected and Automated Vehicles (CAVs).
- In terms of quantum computing, Finland announced the making of their first quantum computer; UK launched the National Quantum Computing Centre.
- Australia has launched a national block chain roadmap.

# Digital Economy

Digital economy and taxation were topics much discussed in 2020.

The importance of cooperation in the digital economy was highlighted in the report released by the European Parliament "Enforcement and cooperation between Member States: E-Commerce and the future Digital Services Act". The United Nations Conference on Trade and Development (UNCTAD), the International Trade Centre (ITC) and the World Trade Organisation (WTO) launched the SDG Trade Monitor to track and provide data on global trade's contribution to the UN sustainable development goals (SDGs). The UN Department of Economic and Social Affairs (UN DESA) published a Compendium of digital government initiatives in response to the COVID-19 pandemic.The Middle East announced their Ten Digital Economy Guidelines for a successful digital economy. The organisations which embraced these guidelines are the Union of Arab Banks (UAB), the Union of Arab Chambers (UAC), International Network for SMEs (INSME), and the Global Coalition for Efficient Logistics (GCEL).

In terms of digital currency, the WEF launched a consortium for digital currency governance, Canada issued guidance for cryptocurrency exchanges and Facebook announced modifications in the Libra cryptocurrency initiative and rebranded it as Diem.

## Taxation

**Challenges over the global tax structures** persisted in 2020, as no clear policy was been agreed upon.

The OECD/G20 released an Inclusive Framework on BEPS,  where they warned that "Disagreement over global digital taxes may result in unilateral taxes and increased trade disputes, triggering a global trade war that could potentially shave off 1% of the global GDP annually" and reiterated the international communities' commitment to address tax challenges arising out of the digital economy.

Owing to COVID-19, the OECD pushed back the target date to reach a global agreement on digital taxation following the US withdrawing participation from the international discussion on global digital tax.  The OECD reiterated their continued commitment to work towards a multilateral agreement on the same.

Further, United Nations released a revised draft proposal for taxation of automated digital services, the UN Committee of Experts on International Cooperation in Tax Matters released a draft tax treaty proposal on payments for digital services and the proposal added a new article to the UN Model Double Taxation Convention between Developed and Developing Countries (UNMC). New Zealand, Canada and Ukraine sought transparency in e-commerce negotiations at the WTO; European Union wrote to the G20 to prioritize digital tax, the G20 meeting ministers backed the revised tax scheme under the framework of G20/OECD by 2020. The UN Committee of Experts on International Cooperation in Tax Matters released a draft tax treaty proposal on payments for digital services and the proposal added a new article to the UN Model Double Taxation Convention between Developed and Developing Countries (UNMC);

Due to the delay in OECD finalising a global taxation policy on online companies, **nations continue to introduce some form of taxation**. Spanish government approved a digital service tax and announced plans to impose a tax on instant messaging providers, Thailand approved a draft legislation to impose 7% value added tax (VAT) on foreign digital companies earning more than 1.8 million baht (US$57 434) per year from digital services in the country. The Czech Republic has agreed to cut the proposed digital services tax to 5% from 7% and delay the tax's effective date to 1 January 2021. Indonesia imposed 10% VAT from July and accelerated digital tax reforms amid the COVID-19 outbreak. France planned to implement a 3% digital tax "Les GAFA'' and announced that online tech platforms will have to pay a 'digital tax' for their 2020 earning. Canada announced plans to levy value added tax over cross border digital products and services, India implemented the 2% Digital Tax, Poland announced plans of implementing a digital tax on online streaming companies and the Kenya Revenue Authority (KRA) sought comments on a proposed digital tax on income from services provided through the digital marketplace which was expected to come into effect on 1 January 2021, requiring individuals and businesses that earn income from services through the digital marketplace to pay a 1.5% tax on the gross transaction value.

Further, Facebook's French subsidiary agreed to pay the French government 106 million euro (US$125 million) in back taxes and penalties for the years 2009-2018; Amazon announced to increase fees for UK sellers by 2% in response to the introduction of the UK's digital services tax, the Executive Vice President of the European Commission, Margrethe Vestager, issued a statement announcing that the European Commission (EC) would appeal the decision of the General Court of the EU that annulled the EC decision of Apple owing Ireland €13 billion in unpaid taxes because of an alleged tax arrangement that had amounted to illegal state aid.

## Digital Trade

In terms of **digital trade,** the G20 Trade and Investment Ministers issued a statement post their virtual meeting highlighting the critical role played by the digital economy and eCommerce during the pandemic; the growing divide among communities who lack access to the digital economy; need for implementing the G20 Action Plan on Trade and Investment to support businesses and workers on the economic recovery from the pandemic.

Fifteen Asia-Pacific countries including China, Australia, Japan, New Zealand, Philippines, and Malaysia signed the Regional Comprehensive Economic Partnership (RCEP), termed as the largest trade agreement in the world. The signatory countries represent about 30% of the world's population, of global GDP, and nearly 28% of global trade. Expected to shape global economics and politics, the RCEP is intended to facilitate international trade by reducing tariffs and administrative requirements among the member states' regulating Telecommunication services, including ICTs, Intellectual property, setting up dispute settlement; E-commerce, etc. India however, withdrew from negotiations last year due to concerns over its domestic industry and the potential of widening trade deficits with member countries, especially China.

Another topic much debated in 2020 was **whether online companies should pay news media and publishing houses for their content**. The Australian Competition and Consumer Commission (ACCC) informed that online platforms such as Facebook and Google will have to pay fair compensation to news media. Facebook declared that it will stop news sharing, if the Australian News Bargaining Code is adopted but would be paying news publishers in the UK. The French competition authority ruled that Google must pay publishing companies and news agencies for reusing content. This was further reiterated by a French court of appeals ordering Google to negotiate with French new publishers about payments for their news content, confirming the decision of the French Competition Authority from 9 April 2020.

Commissions **charged by tech companies** was another topic discussed. South Korean lawmakers called Google to lower its commission for app market purchases amid concerns of local app developers over high fees. In response, Apple announced to reduce its App Store commission rate by 15% for app developers with less than USD$1 million in annual net sales. Google announced postponing the 30 per cent commission on in-app purchases of digital content from its Play Store from next January to next September. Further, Google announced signing of "some individual agreements" on copyright payments to French newspapers and magazines, facing backlash from developers.

## GIG Economy

Due to the pandemic, many businesses, especially startups and SMEs faced the risk of closure due to the economic downturn. The gig workers have been severely hit by the pandemic highlighting the lack of social protection for them. While business of companies such as Uber, travel service providers (Bla Bla car), accommodation providers (AirBnB, Booking.com), airlines and tourism service providers have been affected, the present situation is providing an opportunity to online ecommerce companies and technology companies providing remote meeting services (Zoom, Adobe Connect, Webex, etc), health services providing products and services to fight against the virus.

The argument on the status of ride hailing apps (whether transport operators or information society service providers) and platform workers (employees or independent contractors) continues to be debated with no clear solution. Concerns were also raised on their algorithmic transparency and accountability.

The Court of Justice of the EU (CJEU) Advocate General Szpunar held that a virtual service that puts taxi passengers with taxi drivers in touch is an information society service (ISS); in the US, Uber made changes to align with the new law related to the status of platform workers. Another issue was whether Uber drivers are employees.  The French court has ruled that Uber drivers will be regarded as employees, the general state attorney in Massachusetts sued  Uber and Lyft, alleging that they illegally misclassify their drivers as independent contractors. Voters in California have passed Proposition 22 (Prop 22) that side steps the AB5 bill**,** exempting ride-hailing apps from classifying drivers as employees. The App Drivers and Couriers Union (ADCU) in UK sued Uber for algorithmic accountability.

# 2020 Key APNIC Highlights

This year, APNIC along with WIDE Project, announced establishing the Asia Pacific Internet Development Trust (APIDT) to boost the work of APNIC Foundation especially towards building technical skills and capacity, improving critical Internet infrastructure, supporting research and development, and improving the community's capability in order to build an open, global, stable and secure Internet. Towards this, APNIC conducted the two yearly 2020 APNIC survey, launched a Vulnerability Reporting Program to provide guidance to security researchers who find bugs or weaknesses in any of APNIC's services, released the APNIC Foundation Annual Report for 2019; released the 2020 APNIC survey report, announced the four 2020 ISIF Asia Grant recipients, and organised the APNIC50 conference virtually between 8-10 September.

APNIC analysed the pool of allocated but unadvertised IPv4 address space, which revealed that there were 350,000 unadvertised IPv4 addresses delegated less than five years ago; around 50 million unadvertised IPv4 addresses delegated over five years ago; and around 3.4 million unadvertised and returned historical IPv4 addresses. Few of the potential actions imagined by APNIC include returning them to the original pool, transferring them, or having them managed under the APNIC account.

With several NOGs and technical conferences in the region being cancelled, APNIC initiated a new series of virtual technical events for the Internet operations community called 'Networking from Home' (NFH) which was very well received and attended. The first event was held on 2 June, the second event "Networking from Home South Asia" was held on 17 June, the third Networking from Home (NFH) East Asia was held on 15 July, and the final Networking from Home (NFH) event was held on 4 August following the Oceania time zone.

Further this year, APNIC celebrated the 25th anniversary of APRICOT during APRICOT 2020 and APNIC 49 was held in Melbourne, Australia from 12 – 21 February (with workshops from 12-16 February and conference from 18 – 21).

Pic: 25th Anniversary celebrations of APRICOT (Source:APNIC)

This year, three members were elected to the APNIC Executive Council: Sumon Ahmed Sabir, Achie Atienza and Kam Sze Yeung, while Subham Saran and GM NIXI was elected as the NRO NC. APNIC EC appointed Nicole Chan to NRO NC and Satoru Tsurumaki was selected as a member of the IANA Numbering Services Review Committee (IANA RC)to represent the APNIC region for a two-year term.

APNIC continued its community engagement in events across the region as well as globally. These include participation in : Bangladesh Network Operators Group (bdNOG 11); the Myanmar Internet Exchange and Myanmar Network Operators Group Forum (MMIX MMNOG Forum 2020); the South Asian Network Operators Group (SANOG 35) in Karachi, Pakistan, where Paul Wilson, DG APNIC, presented a keynote emphasising the need to deploy IPv6 and the role of NOGs in Internet development; the GFCE Pacific Regional Meeting 2020 ; GFCE Annual V meeting; the 2020 Global Cybersecurity Capacity Building (GCSC) Conference held in Melbourne, Australia; the DNS Operations, Analysis, and Research Center 32a (DNS OARC 32a) online meeting; the PITA Technical and Business Session where they made a presentation "Cybersecurity outside office in APAN50 supported and participated in the second Cambodia Network Operators Group (KHNOG2), the third Indian Network Operators Group (INNOG3) meeting and the 2020 Open Policy Meeting for the Indian Registry for Internet Names and Numbers (IRINN OPM 2020); in several intergovernmental meetings online;in SIG2020; seventh edition of the Bhutan Network Operators Group (btNOG 7), 12th Bangladesh Network Operators Group (bdNOG 12); Youth IGF India 2020; IGF2020; IETF 109 Bangladesh IGF bdIGF2020; CNX2020; PacNOG 27; APSIG 2020; IDNIC AMM2020 and BSides Brisbane.

APNIC DG Paul Wilson participated and spoke in several events, which include 2020 Taiwan Internet Governance Forum (TWIGF 2020) where he made a presentation on Critical Internet Resources, The Digital Dialogue series on Internet Governance in India,gave a keynote speech at pkSIG2020, in APTLD78; NetThings2020, Cyber Pacific Dialogue, ConnectAsia2020; Connections 2020 and ITU Global Cyber Drill 2020.

# 2020 Key ICANN Highlights

Due to the pandemic, most of ICANN's community members collaborated online, with the three ICANN meetings (67, 68 and 69) held virtually. Some of the topics most discussed this year include: Sale of .ORG, Expedited Policy Development Process and its next phase, WHOIS, Subsequent Procedure, newGTLD round, DNS Abuse and Universal Acceptance.

**This year ICANN:**

- Withheld consent of the proposed sale of the Public Interest Registry (PIR)- .ORG, by Internet Society (ISOC) to Ethos Capital.
- Adopted the FY21-25 Operating and Financial Plan and FY21 Budget that came into effect on 1 July 2020.
- Announced successful installation of ICANN Managed Root Server (IMRS) instances in the Republic of Palau (Palau) and successfully in Monterrey, Mexico along with Transtelco.
- Signed MoUs with Forum of Incident Response and Security Teams Inc (FIRST) on DNS Threats Mitigation, with the Global Cyber Alliance and the Georgian National Communications Commission.
- Released the Domain Name Marketplace Indicators that reflect industry metrics related to gTLDs and ccTLDs through the ICANN Open Data Platform.
- Announced revised policy for the protection of Red Cross & Red Crescent Identifiers; the successful completion of string evaluation of the proposed Internationalized Domain Name (IDN) country code top-level domain (ccTLD) string for Israel and the publication of the fourth version of Label Generation Rules for the Root Zone (RZ-LGR-4).
- Released the first in a series of EU policy papers that will provide EU policy updates and analysis on topics, initiatives, and proposed legislation of potential relevance to the ICANN.
- Responded to the European Commission's public consultation on the Digital Services Act (DSA); the European Commission's (EC) public consultation on the EC's draft Standard Contractual Clauses (SCCs) for transferring personal data to non-European Union (EU) countries.
- Launched the Community Childcare Grants Pilot Program for ICANN68 and the Pandemic Internet Access Program Pilot for ICANN69.
- Announced new travel guidance; support to registrants impacted by the closure and insolvency proceedings against Net4 India.

- Announced the final list of seven selected candidates for the leadership position selected by NomCom; awarded Olivier Crépin-Leblond the 2020 ICANN Community Excellence Award; launched the Dr. Tarek Kamel Award for Capacity Building and Ramanou Biaou was the first recipient of this award.
- In terms of the IANA functions, the ICANN systems controls were validated by annual IANA functions audit conducted by accounting firm RSM US LLP; ICANN and PTI published U.S. Tax Returns for Fiscal Year Ending 30 June 2019; the IANA Naming Function Review Team (IFRT) announced that it has completed the Rules of Engagement, Scope of Work, and Work Plan for the IANA Naming Function Review (IFR).
- Announced the venues for upcoming meetings: ICANN74 Policy Forum to be held in the Hague, Netherlands from 13-16 June 2022; ICANN75, the Annual General Meeting to be held from 17-22 September 2022 at the Kuala Lumpur, Malaysia and ICANN76 at Cancun, Mexico between 11-16 March 2023.
- Appointed Chris Mondini as ICANN Vice President, Stakeholder Engagement, Europe and Managing Director, Brussels and Naella Sarras as the President of Stakeholder Engagement in North America; while ICANN staff Baher Esmat was appointed Managing Director for the Middle East and Africa (MEA) Regional Office.
- Sought comments from the community on the: proposed amendment of the .COM Registry Agreement (RA); the proposed dates for ICANN Public Meetings; Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2; draft proposal for NextGen@ICANN program improvements; Name Collision Analysis Project (NCAP) Study 1; Middle East and Adjoining Countries (MEAC) Strategy 2021-2025; revised community travel support guidelines; Proposal for Chinese Script Root Zone Label Generation Rules; Proposal for Bangla Script Root Zone Label Generation Rules; Public Comment Period of Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report; Phase 1 Initial Report of the Review of All Rights Protection Mechanisms (RPMs) in All gTLDs Policy Development Process (PDP); draft ICANN Africa Regional Plan for Fiscal Years 2021-2015; PTI Strategic Plan fiscal years 2021-2024; Name Collision Analysis Project (NCAP) Study 1 Report; proposal for Malayalam Script Root Zone Label Generation Rules; ccNSO Policy Development Process 3: Initial Proposals for Process to Retire ccTLDs; Latin America and Caribbean (LAC) Regional Strategic Plan for FY 2021-2025; Enhancing the Effectiveness of ICANN's Multistakeholder Model initiative; Label Generation Rules for the Root Zone Version 4 (RZ-LGR-4); GNSO New gTLD Subsequent Procedures Draft Final Report; Reference Label Generation Rulesets (LGRs) for the Second Level; proposed Amendment 1 to the .JOBS Registry Agreement to effectuate a change in the .JOBS TLD Sponsor; IANA naming function review (IFR) initial report and ICANN's root name service strategy and implementation.

Besides, some of the publications from the Office of the CTO (OCTO) include: 5G Technology; New IP; Brief Overview of the Root Server System; DNS Purchasing Guide for Government Procurement Officers; Technical Analysis of the EDPB letter to BEREC; DNSSEC: Securing the DNS and DNS Root Server Operations.

# 2020 Internet Society Highlights

In 2020, all activities of Internet Society were focussed under the overarching mission of: growing the Internet (by building community networks, fostering infrastructure and community development and measuring the Internet), strengthening the Internet (by promoting encryption, the Internet way of networking, Mutually Agreed Norms for Routing Security (MANRS)), encouraging open standards everywhere and promoting Time Security.

This year Internet Society was embroiled in the .ORG sale controversy, where the sale was eventually overturned. Further, Internet Society announced to continue funding the IETF; presented the prestigious Jonathan B. Postel Service Award to Onno W. Purbo. It also launched the Africa Internet Measurements Collaboration along with AFRINIC, created the Internet Impact Assessment Toolkit, released a statement expressing concern over the U.S. Clean Network Program, stating that such policies are likely to increase the global momentum towards a "Splinternet" — a fractured network, set up the Global Encryption Coalition along with the Center for Democracy & Technology (CDT) and Global Partners Digital, to promote and defend encryption in key countries and multilateral gatherings, which has been supported by more than 36 civil society organizations including CCAOI. An open letter has been sent to the Ministry of Electronics and IT, Government of India over concerns related to the draft Intermediary Rules, especially related to breaking encryption; announced the commitment of more than 300 network operators to the MANRS, partnered with the European Internet Exchange Association (Euro-IX) to build on existing collaboration between the two organizations, signed an MoU with Association for Progressive Communications (APC) to work together on designing and deploying community networks, released the Action Plan 2021 that focuses on the need to grow the internet by building community networks, foster infrastructure and community development and measuring the Internet, make the internet stronger by promoting the Internet Way of Networking, extending Encryption, securing the global routing and preserving the Open Internet model, and need to empower people by supporting community participation, building expertise and capacity and securing resources for growth and greater impact.

This year, Ndeye Maimouna Diop and George Sadowsky were elected from the Chapters and Ted Hardie was elected as the organisational members as the ISOC Board of Trustees 2020. Chris Wilson, Amazon; Harald Summa, DE-CIX and Chris Hemmerlein, Facebook were appointed as the new Organisation Members Advisory Council (OMAC) Co-Chairs for 2020 – 2022, representing the organisational members of Internet Society. The OMAC serves as an advisory body to the Internet Society President and Board of Trustees.

Some of the papers and reports released by Internet Society this year includes: Major initiatives in Cybersecurity: Public and Private contributions towards increasing cybersecurity; the Internet

Society 2019 Impact Report,  An analysis of the ‘New IP’ proposal to the ITU-T’, the 2020 Indigenous Connectivity Summit Policy Recommendations for North American indigenous people.

The Internet Society Foundation announced $1.5 million USD in COVID-19 response grants and the seventeen new recipients who were awarded Beyond The Net Large Grants, announced the launch of a new research grant project that sought proposals on Greening the Internet and The Internet Economy.

In terms of Chapter activities, the  Internet Society organised webinars and online discussions on the  2020 Global action plan, the InterCommunity discussion on Open Standards Everywhere, virtual roundtables on ISOCs strategic goals, securing the global routing system, about fostering Infrastructure and Technical Communities, a virtual social event ISOC@ ICANN and a community update on their Internet Growth projects.  It also initiated community consultations on the  Shape Action Plan 2021, Internet Society Community Learning Needs, invited applications from chapters or the Chapterthon2020 which was themed “I heart the internet”; invited comments on the  World Telecommunications/ICT Policy Forum (WTPF)Â preparatory process for the next WTPF meeting in 2021 and feedback on the Internet Way of Networking (IWN) project.

## Updates from APAC Bureau:

This year the APAC Bureau engaged with regional, governmental, intergovernmental and other organisations, participated in events such as APRICOT2020, APrIGF2020, APNIC, Community Network Exchange 2020 (CNX2020), organized informal meet-up at APRICOT2020, organised several online discussions that were aligned to the action plan of Internet Society including, regional calls to discuss the Regional Activities for 2020, forces affecting the Internet [Trends 2020] Trends 2020, discussions related to encryption, fake news, intermediary liability, internet exchanges and MANRS, sessions to provide an overview on encryption and Indian scenario, a call with the Indian Chapters and community members on Encryption and Intermediary Liability in India, a discussion on Kids the Internet and Covid-19: How to keep our children safe online”, discussion on “Encryption after COVID-19: Whats coming up in Asia Pacific”, collaborative virtual meeting with Asia Pacific Internet Exchange Association (APIX);  webinars «True Lies: Misinformation, Censorship and the Open Internet»; ‘How Community Networks are helping during COVID-19’; made submission on “Inviting suggestions on Strategy for National Open Digital Ecosystems (NODE)” to the Ministry of Electronics and IT (MeitY) Government of India; organized the Asia Pacific Virtual Chapter Workshop 2020 this month which was attended by 70 chapter members from 19 economies.

■■■

# 2020: Indian Tech Policy Update

Despite the pandemic, there were several developments in the Indian Tech Policy arena in 2020. Tech geopolitics: banning of apps and making changes in FDI policy; draft data protection bill; draft non personal data bill; liability of intermediaries especially in managing content, regulating hate speech and their growing market power; concerns related to cyber security and privacy concerns associated to contact tracing apps, were much discussed.

We from CCAOI have listed some of the month wise developments of 2020 below:

## January

- Competition Commission of India (CCI) published a 'Market Study on e-Commerce'.
- Niti Aayog released a discussion paper "Blockchain: The India Strategy" recommending Reserve Bank of India(RBI) to issue a central bank digital currency.
- NITI Aayog released the National Data and Analytics Platform Vision Document.
- The Internet and Mobile Association of India (IAMAI) announced the "Self Regulation for Online Curated Content Providers" naming Hotstar, Voot, Jio, and SonyLiv as signatories. Amazon, Netflix are however not part of this initiative.
- The Ministry of External Affairs set up a new division called New, Emerging and Strategic Technologies (NEST) to act as a nodal agency for issues pertaining to emerging technologies.
- The Supreme Court pronounced that the indefinite internet restrictions in Jammu and Kashmir are against the constitution.
- To prevent sexual abuse of children online and access to online child sexual abuse material (CSAM), a fourteen-member adhoc committee made forty recommendations.
- The Joint Select Committee (JSC) reviewing the draft Data Protection Bill (PDP Bill) sought comments on the bill.

## February

- The Supreme Court struck down the crypto ban implemented by the RBI in 1981.
- Inflight Wi-Fi to be allowed within the country.

- Government set up a twelve member "Technology group" to provide policy and strategic advice on new technologies.
- Ecommerce companies sought more time to implement the 1% tax deduction at source (TDS) levy.
- Competition Commission of India (CCI) ordered a probe into anti-competitive allegations against MakeMyTrip and Oyo.

## March

- Ministry of Electronics and Information Technology (MeitY) invited comments on the Strategy for National Open Digital Ecosystems (NODE)
- There was news that MEITY has started consultations on amending the Information Technology Act, 2000.
- CCI invited comments on the on the Competition (Amendment) Bill, 2020
- The Supreme Court did away with the RBI circular that prevented banks from trading in cryptocurrencies.
- Big tech companies sought a deferment of the new Indian digital tax (equalization levy) of 2%, which came into effect from 1 April 2020, due to shrinking business owing to the Coronavirus pandemic.
- Due to COVID-19, in India the mobile date usage increased by 16% while the average network peak hour went down by 36%. To manage this surge in data traffic, telcos urged subscribers to use data networks responsibly.
- The Aarogya Setu contact tracing mobile app was introduced by the government to track COVID-19 cases.
- MeitY issued an advisory for social media companies to initiate awareness campaigns on their platform against such false news, take immediate action and disable, remove such content on priority and disseminate authentic information related to coronavirus.
- The Indian Government issued a set of guidelines for telemedicine.

## April

- The Indian government announced changes in the foreign direct investment rules to curb "opportunistic takeovers/acquisitions" from any entity that shares a land border with India during COVID-19. It is widely seen as a move to prevent takeovers by Chinese firms during the crisis. Under the new rule, entities would be required to obtain government approval for any investment or transfer of ownership of Indian companies arising out of FDI investments.

- Facebook bought a 9.9% stake in Reliance Jio for $5.7 billion. Apart from this investment, Jio Platforms, Reliance Retail and WhatsApp entered into a commercial agreement whereby Whatsapp would be used to further accelerate Jio's ecommerce business and is believed to help in the launch of WhatsApp pay in India.
- MeitY asked Indian companies to develop an encrypted video conferencing solution and even announced funding for the winner .
- The cyber-security chief issued cyber-advisory for online users .
- The Data security Council of India (DSCI) issued an advisory for hospitals and health care industry to fight Covid-19 related cyberattacks.

## May

- The government published the draft social media advertisement policy guidelines for government ministries and departments.
- Government asked ISPs to block We Transfer citing "interest of national security or public interest".
- An antitrust complaint was filed against Google over unfair promotion of Google Pay on Android Play Store.
- Competition Commission of India initiated a review over allegations that WhatsApp is abusing its dominant position by offering payment services to its app users.
- A petition was filed against Twitter at the Supreme Court seeking the government to create a mechanism to check content and advertisements on Twitter which allegedly spread hatred and are " against the spirit of the Union of India".
- The source code of Aarogya Setu app was made available in GitHub and the government has also announced a bug bounty program.

## June

- The government imposed a ban on 59 Chinese apps invoking section 69A of the IT Act.
- CCI approved Facebook's purchase of a stake in Jio Platform.
- It is reported that CCI has initiated a study on the telecom sector and merger and acquisition in the digital market.
- In a case filed by Paytm alleging that telecom operators are blocking "phishing" activities over various mobile networks, TRAI has termed the allegation of Paytm "misconceived".
- At the Delhi High Court, where Google Pay has been accused of not having required authorisation from the RBI to operate, RBI clarified that Google Pay is not a payments system operator, nor has it violated the Payments & Settlements Act.

- The Ministry of Civil Aviation invited comments on the draft Unmanned Aircraft System Rules, 2020 (UAS Rules) policy .
- The I&B ministry proposed to bring OTT content which is managed by MeitY under their preview.

## July

- The Expert Committee on Non-Personal Data Governance Framework invited comments on the "Report by the Committee of Experts on Non-Personal Data Governance Framework".
- The Consumer Protection Act 2019 came into force.
- Google announced buying 7.73% stake in Jio Platforms for $4.5 billion as part of its recently announced $10 billion India digitisation fund.
- Reliance Jio and Google entered into a commercial agreement to jointly develop entry-level affordable smartphones.
- CBIC & CBDT signed an MoU to facilitate smoother bilateral exchange of data.
- The Department of Telecommunications ordered telecom operators to record the GPS coordinates of bulk subscribers who purchase ten or more connections simultaneously.
- The government released guidelines for online education.
- As per government directive, e-commerce platforms would have to mandatorily display the country of origin for all imported products.

## August

- India celebrated 25 years of the Internet in the country on 15 August.
- The government banned another 118 Chinese Apps.
- The submarine optical fibre connecting Chennai to Port Blair and few more islands was inaugurated.
- The Supreme Court ordered telcos to pay their adjusted gross revenue (AGR) in 10 years, (by March 2031).
- The Parliamentary Standing Committee on Information Technology discussed ways to minimise internet shutdowns and prioritise more logical ways to order an internet shutdown and in that context, the committee questioned the Department of Telecom on Internet shutdowns and 5G preparedness.
- The Joint Select Committee on the Data Protection Bill heard presentations from the Associated Chambers of Commerce and Industry of India (ASSOCHAM) and the APJ Abdul Kalam Centre, Facebook and other companies.

- MeitY launched "Swadeshi Microprocessor Challenge- Innovate Solutions for #Aatmanirbhar Bharat" to provide further impetus to the strong ecosystem of Start-up, innovation and research in the country.
- Industry association IAMAI proposed an ombudsman model for OTT streaming regulation.
- eCommerce industry associations sought 6-7 months to comply with the new Consumer Protection (E-commerce) Rules, 2020, that includes e-tailers to mandatorily display the 'country of origin' of goods, and appoint grievance officers.
- The RBI sought comments on the "Draft framework for recognition of a Self-Regulatory Organisation for Payment System Operators.
- Comments were invited in the draft Health Data Management Policy under the National Digital Health Mission.
- The RBI released Draft Framework for authorisation of a pan-India New Umbrella Entity (NUE) for Retail Payment Systems.
- It was reported that online beauty and fashion portal Nykaa was duped of Rs 62 lakhs by cybercriminals.
- It was reported that PayTM Mall suffered a data breach with attackers demanding a ransom in cryptocurrency in exchange of the data, the company however has denied the attack.

## September

- MeitY met with startup founders to understand their concerns over the 30% fee Google would be charging for digital goods and services in India and other concerns related to the Tech Giant.
- 120 Indian startups formed an indigenous app developers' association to lobby against global technology giants.
- Vodafone won an international arbitration against India in $2 billion tax dispute case.
- Google applied to the CCI to approve the deal with Reliance Jio.
- Amazon sent legal notice to Future Group over Reliance deal.
- Tamil Nadu released their Cybersecurity Policy.
- The names of the reconstituted Parliamentary Committee of Information Technology members were announced with Shashi Tharoor to chair the committee.
- Dr. PD Vaghela was appointed the chairperson of the Telecom Regulatory Authority of India (TRAI).
- NITI Aayog sought public comments on the draft Data Empowerment and Protection Architecture (DEPA).

## October

- The Delhi High Court ordered social media platforms to take adequate measure to ensure child sexual abuse content is not hosted in their platforms.

- The industry associations representing the cloud services providers such as Amazon Web Services, Google Cloud and IBM wrote to the Department of Telecom (DOT) in relation to the new TRAI regulation of the cloud service industry to be required to join an industry association created by the DOT. They termed this recommendation as overstepping the jurisdiction of MeitY and overbearing.

- The parliamentary standing committee on IT met the telcos to discuss and assess India's 5G readiness and representatives of the Home Ministry and Delhi and Bihar state governments to understand the effectiveness or shortfall of internet shutdowns.

- To streamline the spectrum allocation process, the government constituted a panel of secretaries (home, defence, railways, telecom, I&B and department of space) under cabinet secretary Rajiv Gauba.

- The government modified the work from home (WFH) and Work From Anywhere (WFA) guidelines for companies, which is expected to benefit the IT industry, primarily the business process outsourcing (BPO) sector.

- The government published 'clarification' on 26% FDI in digital news media.

- The government issued a clarification on the creator of the COVID-19 contract tracing app Aarogya Setu after the Central Information Commission (CIC) issued show-cause notice to government departments asking who had created the app.

- A group of digital media platforms such as OpIndia, Goa Chronicle and Republic World formed a self regulatory Indian Digital Media Association (IDMA).

- The Supreme Court refused to hear a plea filed by the CCI,seeking to remove a Karnataka High Court-directed stay on its probe against Amazon and Flipkart. Instead, the apex court directed the Karnataka High Court to decide on the matter within six weeks. It may be mentioned that had ordered a probe into alleged competition law violations by Amazon and Flipkart on January 13.

- The Registrar of Copyrights invited comments privately from select industry stakeholders on the Copyright Act, indicating that the government may soon make amendments to it.

- NITI Aayog released a draft discussion paper 'Designing the Future of Dispute Resolution: The ODR Policy Plan for India'.

- Market regulator Securities and Exchange Board of India (SEBI) constituted a Market Data Advisory Committee (MDAC) for recommending policy on Market Data Access.

- The Joint Parliamentary Committee on Personal Data Protection met representatives of several companies including Facebook, Amazon, Twitter, Google, Paytm, RelianceJio, cab aggregators (Ola and Uber) on issues related to privacy and data protection in their platforms.

- CCI initiated investigations over Google's abuse in smart TVs market.
- Several Indian startup founders such as Paytm, BharatMatrimony, MayMyIndia, etc. met the CCI with concerns over Google's dominance.
- Cyberattack on Indian drug maker Dr Reddy Laboratories Ltd
- Ransomware attack on Press Trust of India's operation.
- India joined the "Five Eyes" group of nations and Japan to release a joint international statement against encrypted social media platforms, urging the companies not to overlook illegal activities including the sharing of child abuse content on their platforms
- The Delhi High Court in India, ordered social media platforms to take adequate measure to ensure child sexual abuse content is not hosted in their platforms.
- Google, Netflix, Adobe agreed to pay up 2 per cent additional equalisation levy levied on digital companies. Amazon decided to pass on the equilisation levy to the consumers.

## November

- The CCI initiated investigations over Google's abuse of its dominant position in its app store to promote its payments services Google Pay.
- The government banned another 43 Chinese mobile applications citing security concerns, taking the tally of banned Chinese apps in India to 267.
- The Indian government capped the surge pricing to 1.5x and commissions to 20% of cab aggregators such as Uber and Ola.
- CERT-In issued advisory for companies against new ransomware.
- CCI approved Google purchasing 7.73% stake in Jio Platforms and thereby cleared the way for the internet giant to jointly develop entry level Android smartphones.
- Facing backlash, the government of Kerala withdrew the ordinance enforcing its criminalisation of online defamation.
- Tamil Nadu banned online gambling in the state; India's 5G technology TSDSI 5Gi completed the evaluation phase of ITU and now conforms with the ITU performance requirement.
- The legal dispute between Amazon and Reliance Industries over the purchase of Future Retail Ltd continues with the case being fought between Future Retail and Amazon in the Delhi High Courts. While the Singapore Arbitration court had halted the sale, the CCI approved the proposed sale.
- MeitY invited comments on the draft Data Center Policy.
- WhatsApp announced the launch of money transfer operation in its platform in India after the National Payments Corporation of India (NPCI) gave its nod to offer payments

services via the Unified Payments Interface (UPI). The service would be available in 10 Indian languages. NPCI has allowed WhatsApp to expand its operation in a graded manner and in the first phase can only expand its payment services to 20 million users.

- Concerns of low broadband penetration especially in rural India persists. As per a report by Deloitte, the broadband penetration in India's rural areas continues to be poor at 29.1% against national average of 51% with 687 million subscribers as of March 2020.
- Niti Ayog has invited comments on the Draft Discussion of the Working Document: Enforcement Mechanisms for Responsible#AIforAll by 15 January 2020
- RBI to set up the Reserve Bank Innovation Hub (RBIH) to promote innovation across the financial sector by leveraging technology and creating an environment to facilitate and foster innovation.

## December

- NITI Aayog proposed setting up of a self-regulatory organisation to be governed by the independent oversight board while restricting the availability of online fantasy games to users of 18 years and above as part of the uniform national-level regulations for the online fantasy sports platforms in India.
- RBI enhances contactless card limit to Rs. 5000 effective Jan 2021.
- Streaming platforms to on-board legal luminaries to bolster self-regulation code.
- The Delhi High court refused to intervene in the Amazon- Future Retail dispute.
- The Cabinet approved setting up of Public Wi-Fi Networks under "PM-WANI" by Public Data Office Aggregators to provide public Wi-Fi service through Public Data Offices without levy of any License Fee.
- To improve police accountability, the Supreme Court has stated that every police station in the country should be equipped with night-vision Closed-Circuit Television (CCTV) cameras, having both audio and video recording capability.
- The Aviation Ministry addressed data security and privacy in a draft policy for unmanned drones. The Ministry of Civil Aviation has released the Draft National Unmanned Aircraft System (UAS) Traffic Management Policy.
- Indian Reserve Bank proposed security controls for digital payments.
- The government announced a National Security Directive on the Telecom Sector for secure networks.
- The Expert Committee has released the revised "Report by the Committee of Experts on Non-Personal Data Governance Framework" for public comments till 27 January 2021.

The updates related to the Telecom Regulatory Authority of India (TRAI) can be viewed in the next section.

# TRAI Updates

The Telecom subscription data of 31 October, 2020 released by the Telecom Regulatory Authority of India (TRAI) indicates that while Internet subscribers especially broadband is in the rise (734.82 million in October, 2020 from 661.938 million in December 2019), the telecom subscribers are coming down (1171.80 in October, 2020 from 1172.4 in December, 2019).

**This year TRAI**

- Issued directions to implement Green Technology in the Telecom Sector and submission of the Carbon Footprint Report to all basic, CMTS, UASL, Unified License & UL (VNO) Licensees; international long distance service providers, internet service providers, national long distance service providers; implementation of The Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018; for minimum threshold of rupees ten to be applicable for generating unique porting code, raising of Non Payment Disconnection requests and reconnection of mobile numbers; directions on tariff publication and advertisements and seeking information related to segmented offers.

- Issued Regulation on the Telecommunication Consumers Education and Protection Fund (Fifth Amendment) Regulations, 2020; Telecommunication Interconnection Usage Charges (Sixteenth Amendment) Regulations, 2020; telecommunication interconnection (Second Amendment) regulations, 2020 and Telecom Consumers Protection (Eleventh Amendment) Regulations (TCPR) 2020.

- Released recommendations on ''Reforming the Guidelines on Transfer Mergers of Telecom Licenses''; Ensuring Adequate Numbering Resources for Fixed Line and Mobile Service; Network Testing Before Commercial Launch of Services for Wireline Access Services; Provision of Cellular Backhaul Connectivity via Satellite Through VSAT Under Commercial VSAT CUG Service Authorization; Methodology of applying Spectrum Usage Charges (SUC) under the weighted average method of SUC assessment, in cases of Spectrum Sharing; Regulatory framework for over-the-top (OTT) communications services; Cloud Services; Traffic management practices (TMPs) and multistakeholder body for Net Neutrality.

- Released the draft Telecommunication Tariff (65th Amendment) Order, 2020 on ''Regulation of tariff for Short Message Service''; Telecommunication Tariff (Sixty Fifth Amendment) order 2020; Telecommunication Tariff (Sixty Fifth Amendment) order 2020 and amendment and clarification to direction on tariff publications.
- Made changes to telecom interconnection rules for fixed line networks.
- Released white Paper on -Smart Cities in India: Framework for ICT Infrastructure;
- Issued advisory for exercising due care while joining online conferences through audio calls for bill shocks.
- Released reports including: Monthly Telecom Subscription Reports (November, 2019, December, 2019, January 2020, February 2020, March, 2020, April, 2020, May, 2020 , June 2020, July 2020, August 2020, September2020, October 2020); Quarter wise Indian telecom Service performance indicator reports(ending September, 2019, December, 2019, March 2020, June 2020); annual report of TRAI for the year 2018-19; report on activities for the year 2019, that highlights all the consultations, recommendations, regulations, orders and directions taken by the regulator in 2019.
- Blocked the faster data speeds and priority services of Bharti Airtel and Vodafone Idea, citing such schemes could lower the quality of mobile services for other users who have not opted for such services, post questioning the two telcos on their stance on differential data speeds, the Regulator issued a show cause notice to Vodafone Idea. Vodafone Idea later dropped the faster data speed claim in their plan.
- The Regulator imposed penalties collectively amounting to Rs 35 crore on eight operators including Bharti Airtel, Vodafone Idea (Vi) and Reliance Jio for allowing cybercriminals to issue fake SMSes to dupe digital payment users.
- Released consultation papers on: Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality; Transparency in Publishing of Tariff Offers; Provision of Cellular backhaul connectivity via Satellite through VSAT under commercial VSAT CUG Service Authorization; Tariff Issues of Telecom Service; Paper on Methodology of applying SUC under the weighted average method of SUC assessment, in cases of Spectrum Sharing; Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services; Regulation of International Mobile Roaming Services; Roadmap to Promote Broadband Connectivity and Enhanced Broadband Speed; Enabling Unbundling of Different Layers Through Differential Licensing; Review of The Quality of Service (Code of Practice for Metering and Billing Accuracy) Regulations, 2006
- Implemented an eOffice.
- Launched the complaint management system (CMS) portal and app.

- Conducted webinars and discussions (example: on ‘5G in India - Specification, Use cases, Challenges and Action Plan and 5G in India - Specification, Use cases; Challenges and Action plan; Methodology of applying SUC under the weighted average method of SUC assessment, in cases of Spectrum Sharing; with ITU and GSMA on ‘Digital Transformation for Digital Economies @COVID-19 South-Asia; 5G - Architecture, Use cases and Govt. Initiatives and IoT - Trends, Security Challenges and Solutions; Cyber Security;

- For the Broadcasting sector, the regulator released a press note on NTO 2.0 highlighting how it provides freedom to stakeholders to price their services while ensuring freedom of choice to consumers; released the implementation of Telecommunication (Broadcasting and Cable) Services (Eighth) (Addressable Systems) Tariff (Second Amendment) Order, 2020; released the recommendations of the Review of Television Audience Measurement and Rating System in India and interoperability of set-top boxes and reserve price for auction of FM radio channels; launched a Channel Selector App to facilitate subscribers to view and modify their TV subscription; issued direction to all broadcasters to ensure compliance of various provision of the Telecommunication (Broadcasting and Cable) Services (Eighth) (Addressable Systems) Tariff (Second Amendment) Order, 2020 and The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Second Amendment) Regulations, 2020; issued amendment to direction dated 24.07.2020 issued to all Broadcasters under Section 13; conducted an open house discussion on Framework for Technical Compliance of CAS and SMS for Broadcasting & Cable Services and released consultation Paper on MIB back reference on TRAI’s Recommendations dated 19.11.2014 on ‘Regulatory Framework for Platform Services’ & MIB reference on TRAI’s Recommendations on ‘Platform Services offered by DTH Operators’ dated 13.11.2019

# Overview of CCAOI Activities in 2020

Most of CCAOI's activities were held online owing to the pandemic. These include organizing and participating in online discussions both within the country and outside, making submissions (e.g. to the Joint Parliamentary Committee on Personal Data Protection; TRAI on Tariff Issues of Telecom Services; Department of Telecom on New Framework for IP; Committee of experts on Non Personal Data Governance Framework, National Open Digital Ecosystem (NODE)), co-authoring reports, disseminating information about policy updates and events related to digital developments through our monthly newsletters and building capacity among the community on internet and relevant policy issues. In 2020, CCAOI joined the Global Encryption Coalition.

## Webinar on the Draft Personal Data Protection Bill

CCAOI along with the support of the Internet Society India Delhi Chapter and The Perspective conducted a second online stakeholder discussion on the Draft Personal Data Protection Bill. The objective of the webinar was to provide the community a better understanding of the bill, seek suggestions and encourage interested community members to make submission to the Joint Parliamentary Committee (JPC). The session was moderated by Amrita Choudhury and the experts who lead the discussion include, Rahul Sharma (The Perspective) Bishakha Bhattacharya (IBM), Belson D (Cognizant Technology), Anu Acharya (Mapmygenome), Shivam Satnani (TCS), Rakesh Jha (Privacy Virtuso), Vinay Kesari (Setu) and Nikhil Pahwa (Medianama). Attended by over seventy-five stakeholders, the recording of the webinar can be heard using this link.

## Co-organised three sessions on Internet Governance

CCAOI co-organised with The Broadband India Forum (BIF) and Bharat Exhibitions (BE), TDSI and with ICRIER as Knowledge Partner organized **The Digital Dialogues (TDD)™ series on Internet Governance.** This series of TDD was focused towards building awareness among the Indian stakeholders on key aspects of Internet Governance, the different actors involved, key issues and concerns being globally discussed and opportunities for the community to participate.

There were three sessions in the series and all the sessions witnessed over hundred participants each, both from within the country and overseas.

The first session "Introduction to Internet Governance: Actors, Issues, Trends & Opportunities" was organized on 29 June. The speakers at the session were: Mr. Chengetai Masango, Head of the United Nations Internet Governance Forum (IGF) Secretariat; Mr. Jovan Kurbalija, Director of Diplo Foundation and Head of the Geneva Internet Platform, Ms. Ankhi Das, Director - Public Policy, Facebook.

The second session "Role of Internet Governance Platforms: ICANN & Internet Society (ISOC)/ IETF" was organized on 2 July. The speakers at the session were: Dr. Gulshan Rai, Distinguished Fellow, Observer Research Foundation (ORF), Mr. Samiran Gupta, India Head, ICANN, Mr. Rajnesh Singh, , Regional Vice President, Asia-Pacific Internet Society, Mr. T Santhosh, Scientist E, Ministry of Electronics and Information Technology (MeitY), Government of India; Mr. Anupam Agrawal, Chair India Internet Foundation (IIFON), Mr. Molay Ghosh, General Manager, JIO Network Planning & Architecture Reliance Jio.

The third session of the series "Introduction to Internet Governance Platform: Asia Pacific Network Information Centre (APNIC)", was organized on 6 July. The speakers at the session were: Mr. Paul Wilson, Director General, APNIC, Mr. K Ramchand, Member (T), Department of Telecommunications (DOT), Mr. Sanjay Goel, Joint Secretary, MeitY and CEO, National Internet Exchange of India (NIXI) and Mr. Ramesh Chandra, Vice President – Network Planning & Engineering, Reliance Jio.

The introductory session was moderated by Dr. Rajat Kathuria, Director and Chief Executive, ICRIER and the subsequent sessions by Mr. Rajat Mukerji, Director General BIF. For all the sessions, Mr. T.V.Ramachandran, President BIF provided the initial remarks and key takeaways of the earlier sessions, Ms. Amrita Choudhury, Director, CCAOI, provided an overview and context to the discussion and Mr. Shashi Dharan from BE, provided the vote of thanks.

The key takeaways from the stimulating discussion series on Internet Governance, from India's perspective were:

- It is essential to reassess the existing Internet Governance views both from domestic and international perspective in the light of the emerging technologies and the geo-political situation.
- India needs to adopt different approaches between domestic and global strategies on Internet Governance.
- Need for enhancing digital cooperation among all stakeholders, both at the national and global level for ensuring the objectives of India are met.
- Initiate a dialogue to start a National Internet Governance Forum (India IGF) for initiating discussions within the country on issues pertinent to India and then develop a national point of view in a very inclusive manner that could be articulated in regional and global IG forums.
- Need to organize more such capacity building sessions, technical workshops to build understanding among community members on technology, digital policies and issues, which in turn would improve greater participation from the community at the national and global level.

- Role of the Industry and Academia needs to be enhanced significantly in standard setting bodies such as IETF for developing standards that are in India's interest.
- Enhance stakeholder participation especially of industry in Internet Governance platforms and their policy development processes would be in India's strategic interest.
- India has an opportunity to bid for hosting the future Global Internet Governance Forum such as for 2024, since the venue is yet to be finalized and proposals for hosting the same are being invited.
- India should try to host an IETF meeting in India to enable more focus towards standard setting.

## Webinar on the draft Non-Personal Data Governance Framework

CCAOI, The Perspective and ISOC Delhi, organised an online discussion on the draft Non-Personal Data Governance Framework. The session was well attended by over hundred participants belonging to different stakeholder communities from across the country.

Moderated by Rahul Sharma and Amrita Choudhury, the panel comprised of experts: Abhishek Singh, CEO, MyGov, Ministry of Electronics & Information Technology, Govt of India; Smriti Parsheera, Researcher, National Institute of Public Finance and Policy (NIPFP) & Fellow, CyberBrics Project; Ashish Aggarwal, Senior Director & Head- Policy Advocacy, NASSCOM; Parminder Jeet Singh, Executive Director, IT for Change (member of NPD committee) and Subhashish Bhadra, Principal Beneficial Technology, Omidyar Network who shared their perspectives on various issues such as data governance, non- personal data and the draft framework.

As Parliamentarian Tejaswi Surya could not attend the discussion, his recorded views on the topic were shared with the audience.

The **detailed summary report** along with the hosts comments on the draft can be viewed using this link. The recording of the session can be viewed using this link.

## CCAOI@AprIGF

CCAOI Director Amrita Choudhury moderated a discussion "Breaking Encryption: Is it the Panacea for addressing security issues online?" organized by Internet Society Delhi Chapter at the Asia Pacific Internet Governance Forum (AprIGF). The speakers in the session were: Rajnesh Singh, Internet Society, Nikhil Pahwa, Medianama; Raman Jeet Singh Chima, Access Now; Jaewon Son, Youth 4IG. Over 58 people attended this interactive discussion.

Some of the key outcomes from the discussion were:

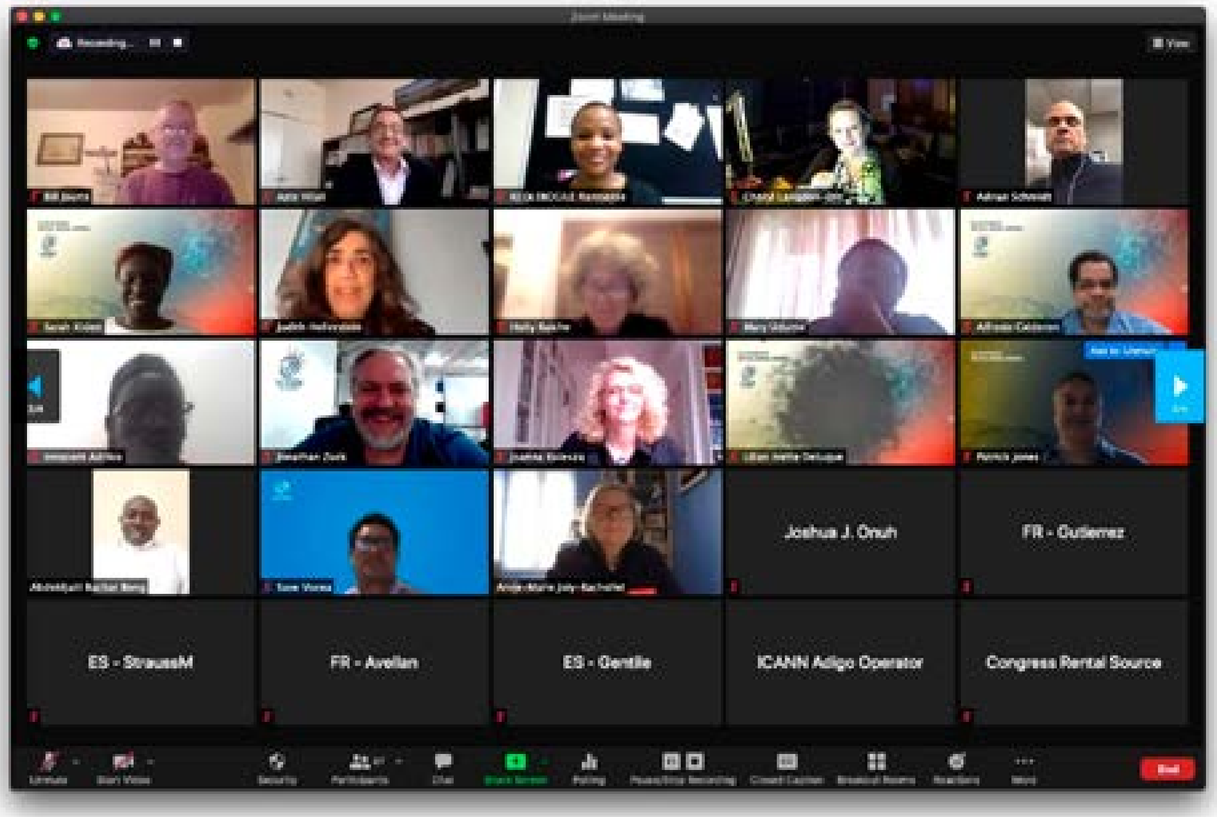
- Breaking encryption or creating exceptional access would not solve the threat of terrorism or eliminate child exploitation and misinformation online. Rather it would have the opposite effect of exposing more Internet users to criminals by weakening the overall security of networks.

- The threat of bad behaviour, which constitutes a comparatively small fraction of activities that people do online, should not define rules for everyone.
- There is a need for a robust encryption policy to ensure that everyone has access to secure communication amidst the continuing rise in cyberattacks globally.
- Concerns were raised over the lack of transparency, accountability and oversight of law enforcement agencies, growing legal or illegal hacking by government agencies, increasing mistrust of citizens on governments and companies.
- To address concerns, there is a need for  deeper discussions; understand the specific concerns related to access of information, whether for intelligence or investigative purposes; build adequate checks and balances related to interception;  there is a need to address the mistrust through dialogue, capacity building and cooperation between stakeholders.
- To address both privacy and security, there is a need to justify the demand for law enforcement access to personal data and communications as well as focused discussions to identify other means to obtain information on criminals without putting people's online activities at risk.
- To mitigate Internet users' loss of confidence amidst proposals to undermine secure communications, encourage more collaboration and dialogue between different stakeholders.
- Greater awareness of privacy is needed, specifically highlighting encryption as a component of online security.

The session can be viewed using this link and a detailed report of the session is available here.

## CCAOI@ICANN69

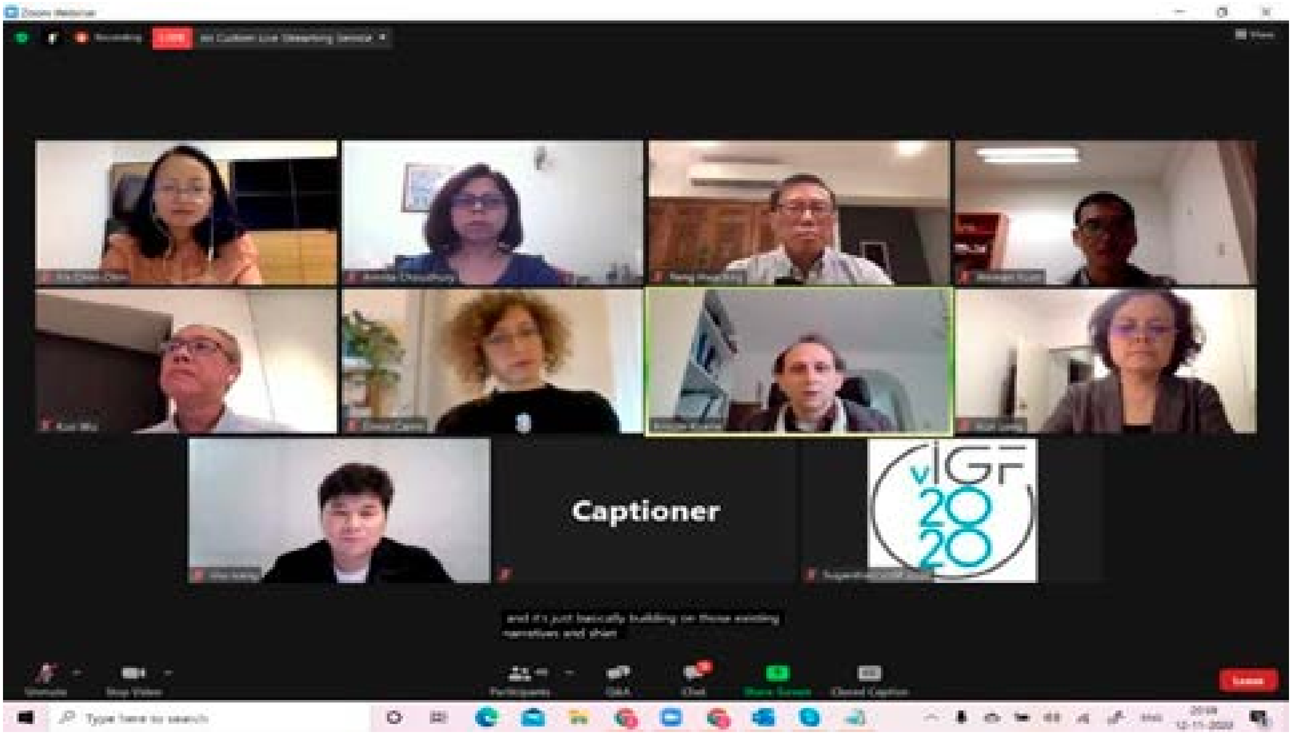
CCAOI organized a pre-ICANN69 session "Ensuring Community Engagement in Pandemic Times'' on behalf of At-Large, showcasing the work done by At Large community members across the globe in spreading the work of ICANN within their communities and contributing back to At Large on the various policy issues with the end user perspective especially during the pandemic. Seventeen ALS members and individual members from the different regions shared their experiences on how they have been engaging and the initiatives they have undertaken within their communities. There was also a discussion on how this engagement can be further improved based on the feedback from ALSes and individual members and also the initiatives being taken by At Large. Recording of the session is available here.



Pic: ICANN69 Session: Ensuring Community Engagement in Pandemic Times

## CCAOI at IGF

CCAOI Director Amrita Choudhury participated and spoke in a session WS108: Trust, Media Ethics & Governance During COVID-19 Crisis highlighting the need to be build the trust deficit online; connect everyone meaningfully; focus on media literacy; need for governments and business to be more transparent about their initiatives; while platforms are taking initiatives to curb the spread of misinformation and hate speech in their platforms, they need to do more transparent on their take down policies, the way their Algorithms take decisions; and need to look at innovative approaches to rebuild trust over internet and it has to be a concerted effort across stakeholders.



and it's just basically building on those existing narratives and then

Pic: IGF Session108

## Co-authored a White Paper on Internet Governance

CCAOI Director Amrita Choudhury and President BIF T. V. Ramachandran co-authored a White Paper 'Internet Governance & Digital Cooperation: A Recommended Way Forward for India' that was released by Broadband India Forum (BIF) at a virtual event to celebrate 25 years of Internet in India. The paper summarizes the discussions of the three The Digital Dialogues series on Internet Governance and the authors' understanding of the action areas from India's perspective on Digital Cooperation, based on the report released by the UN Secretary General.

# Annexure

## Reports & Articles:

Some of the reports and articles published in 2020 include:

- Competition Commission of India has released a report "Market Study of eCommerce in India."
- The World Economic Forum (WEF) has released a report "Cybercrime Prevention Principles for Internet Service Providers"
- Oxfam has released a report " Time to care" that highlights the increasing economic disparity arising due to flawed and sexist economic system that values the wealth of the privileged few, mostly men, more than the billions of hours of the most essential work – the unpaid and underpaid care work done primarily by women and girls around the world.
- BKC has released a report Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights based Approaches to Principles for AI
- SFLC has released their third report in the series on Intermediary Liability called The Future of Intermediary Liability in India.
- The European Data Protection Board has released Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.
- CUTS International has released a report "Consumer Impact Assessment of Data Loacalisation".
- CUTS International has released a report "Competition and Regulation in India 2019".
- ICANN Office of the CTO has released a paper on 5G Technology.
- CISCO released their Annual Broadband Report (2018-2023). The report provides global forecast/analysis and predicts that by 2023, nearly two-thirds (5.3 billion people) of the global population will have Internet access; over 70 percent of the global population will have mobile connectivity; the number of devices connected to IP networks will be more than three times the global population; M2M connections will be half of the global connected devices and connections; connected home applications will have the largest share and connected car will be the fastest growing application type.
- The IANA Numbering Services Review Committee (IANA RC) has published the 2019 IANA Numbering Services Review Committee Report. This report follows a 30-day public

comment period on the IANA Performance Matrix Summary Report published by the RIRs, seeking input from the broader community.

- The World Health Organization (WHO), the United Nations Children's Fund- (UNICEF), and the medical journal group the- Lancet Commission have released a report titled: '"A Future for the world of children" that call on nations to rehaul their approach in protecting the health of adolescent children, their environment, and future.
- UNICEF has released a report, "Our Lives Online: Use of Social Media by Children and Adolescents in East Asia – opportunities, risks and harms." The report highlights that while children benefit by access to the social media sites, this also exposes them to various risks and harms.
- The fourth edition of Inclusive Internet Index 2020 has been released that assesses the performance of 100 countries in four categories of inclusion: accessibility, affordability, relevance, and readiness. This edition of the report focuses on the digital economy.
- GSMA, in collaboration with the International Telecommunication Union has published the'Guidance for ICT Companies Setting Science Based Targets'.
- The Youth and Media (YaM) have released a report "Youth and Digital Citizenship+(Plus): Understanding Skills for a Digital World" that explores aspects of young people and the digital environment and the concept of digital citizenship.
- CUTS International has published a discussion paper on 'Artificial Intelligence: Implication for Consumers' that assesses the benefits and cost of AI for consumers, highlighting the Concepts Related to AI, current Application and Potential Benefits for Consumers, Challenges and Risks – involved along with a set of recommendations.
- GSMA published 'Connected Women: The Mobile Gender Gap Report 2020' that highlights women in low and middle-income countries (LMICs) now have better access to mobile Internet (around 54%). However, in terms of smartphone ownership the gender divide still persists in LMICs.
- The British Standards Institution (BSI) has published a set of safety requirements called PAS 1881: Assuring safety of automated vehicle trials and testing.
- The UN's open-ended working group on cybersecurity has published the Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security.
- OWEG has published the Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security.
- Access Now has released a guide "Fighting Misinformation and defending free expression during COVID-19: Recommendations for states" that focuses on recommendations for governments, companies, NGOs, and individuals to protect freedom of expression and the right to impart and access information during the COVID-19 pandemic.

- ITU has published the Global ICT Regulatory Outlook 2020 (GIRO20) report. A new tool has been introduced this year called the Benchmark of Fifth Generation Collaborative Regulation (G5 benchmark) that evaluates frameworks against 25 measurable indicators clustered into three tracks: collaboration, policy design principles and G5 toolbox elements. It is expected to help regulators monitor, analyse and compare between countries the evolution of regulation as digital markets mature.

- The UN Economic and Social Commission for Asia and the Pacific (ESCAP) published a policy brief 'The Impact and Policy Responses for COVID-19 in Asia and the Pacific', highlighting the need to step up efforts to 'reduce the digital divide' which have come into greater focus with the introduction of social distancing measures.

- The RAND Corporation has published a report ‹Securing Communications in the Quantum Computing Age›, that explores the risks that future quantum computers could pose to current digital encryption systems used to secure information and communication infrastructures.

- Mary Meekers has released a Corona Virus trends report.

- The American Civil Liberties Union (ACLU) has released a white paper "The limits of location tracking in an epidemic".

- The IAMAI-Nielsen "Digital in India" report indicates that India has over 504 million active internet users, of which 71 million of them (14%) are aged between 5-11 years.

- A4AI published a meaningful connectivity standard to define the dimensions of internet access that matter most to users and to help set new, more ambitious targets for connectivity. They have identified four dimensions for meaningful internet connectivity: regular internet us**e** (daily internet access); an appropriate device **(**access to a smartphone); enough data *(*an unlimited broadband connection at home, or place of work or study) and a fast connection (4G mobile connectivity).

- Verisign has released "The Verisign Domain Name Industry Brief" for the period of Jan – March 2020.

- A report on Information Manipulation on Social Media in MENA has been published that studies the social media influence and manipulation in the MENA region, with special attention to the conspiracy theories surrounding COVID-19.

- Global Network Initiative has released their report GNI Principles of Work that evaluates the corporate practices of companies such as Microsoft and Google.

- Zoom has released a white paper on end-to-end encrypted communication.

- The Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC) has published a research paper Why Gender Matters in International Cyber Security.

- An Access Now has released a report " Two years under the EU GDPR" that highlights the flaws in the enforcement of the EU GDPR.

- The Observer Research Foundation (ORF) published the report 'Gender and the GiG Economy: A qualitative study of Gig platforms for women workers' that examines the existing issues faced by women gig workers in India, in terms of use and privacy policies of some of the platforms they use suggests recommendations for inclusion.

- The International Telecommunication Union (ITU) released the Digital Skills Assessment Guidebook that provides a practical step-by-step tool for national digital skills assessments.

- Public Service International, Friedrich Ebert Foundation, and IT for Change released a report on 'Economic Rights in a Data Based Society' which deals with collective data rights, especially in the context of workers' rights.

- Dvara Research has published a paper "What Do We Know About Women's Mobile Phone Access & Use? A review of evidence".

- GSMA released several reports. These include:

  - Report on 'Digital Dividends in Natural Resource Management' released on world environment day.

  - On digital health 'Digital Health:A health system strengthening tool for developing countries' was launched.

  - Two reports on mobile money operability: Many paths to mobile money interoperability: Selecting the right technical model for your market; and Tracking the journey to mobile money interoperability: Emerging evidence from six markets: Tanzania, Pakistan, Madagascar, Ghana, Jordan and Uganda.

- The European Commission published the 2020 Digital Economy and Society Index (DESI) which monitors the overall digital performance of Europe and tracks the progress of EU countries with respect to their digital competitiveness.

- The African Declaration on Internet Rights and Freedoms (AfDec) Coalition has issued a position paper on developments relating to the COVID-19 pandemic in Africa.

- Tandem research has released a report "A Balancing Act – The Promise and Peril of Big Tech in India". The report identifies four conceptual markers that characterize Big Tech: data centric models, network effects, infrastructural role and civic powers; how big tech is transforming the digital economy and society in India; what should be the policy pathways for the nation; and principles for competing value.

- Australian Government's INSLM has published a report on whether encryption law contains sufficient safeguards.

- The Indian Council for Research on International Economic Relations (ICRIER) in collaboration with Google and NASSCOM released a Report 'Implications of AI on the Indian Economy'.

- The ITU Global Symposium for Regulators (GSR) published a discussion paper "Pandemic in the Internet Age: communications industry response" that analyses key initiatives and lessons learned during the Pandemic.

- The European Data Protection Supervisor (EDPS) released a report on how EU institutions, bodies, and agencies carry out Data Protection Impact Assessments (DPIAs) when processing information that presents a high risk to the rights and freedom of natural persons.

- The K7 Security's Cyber Threat Monitor Report highlighted that Chennai recorded the highest number of cyberattacks in the country during the Q4 2019-20 analysis. Among Tier-I cities, Chennai, Bengaluru, Hyderabad and Kolkata recorded the highest rate of infections, while among the Tier-II cities, Patna registered the highest infection rate at 38% followed by Guwahati, Jammu and Bhubaneswar.

- The Alliance for Affordable Internet (A4AI), has published a published a report that indicates that billions of people are denied meaningful access to the Internet due to the high cost of mobile handsets. A4AI looked at the affordability of mobile devices in 70 low and middle-income countries and found that 2.5 billion of people live in countries where the cost of the cheapest available smartphone is a quarter or more of the average monthly income. In India, where the cost of Internet data is lowest, the price of the cheapest smartphone from Jio constitutes 206% of the average monthly income.

- 2020-Unisys Security Index™ that measures concerns of consumers on issues related to national, personal, financial and internet security around the world revealed that 58% people believe personal safety concerns have seen the largest increase; 41% people are seriously concerned about a data breach while working remotely and 62% are concerned by natural disasters such as pandemics.

  The India findings reveal that 32% are seriously concerned about a data breach while working remotely, reflecting a false sense of security, 82% cited their family's physical health as their key concern in a health crisis like COVID-19 and 83% Indians were reported to be concerned about Identity Theft, making it the topmost security concern.

- Reportlinker.com released their "Global Internet Protocol Version 6 (IPv6) Industry" report that predicts the Global Internet Protocol Version 6 (IPv6) market will reach 33. 9 Billion Units by 2027.

- The ITU has released the 2020 edition of the ITU Handbook for the Collection of Administrative Data on Telecommunications/ICT which provides more than 90 internationally agreed indicators to track global ICT developments, focusing on indicators mainly collected by national regulators from the telecommunication services sector.

- The ITU has released the ITU Manual for Measuring ICT Access and Use by Households and Individuals which is a practical tool to guide countries in their ICT data production, serving as a basic reference when preparing, designing and implementing ICT household surveys.

- ITU has released a report "Women, ICT and emergency telecommunications: opportunities and constraints" that explores how through "culturally sensitive inclusion", women can take the benefit of information and communications technology (ICT) and become equal stakeholders in society.

- Omidyar Network India (ONI) and Boston Consulting Group (BCG), had conducted a study and then released a report "Building India's Digital Highway- The Potential of Digital Ecosystems", on their observations "that highlights undertaken a study to reimagine digital platforms for the public good.

- A report "Protecting Workers in the Digital Platform Economy" released by the Indian Federation of App-based Transport workers (IFAT) and the International Transport Workers Federation highlights the health hazards, lack of social security and support faced by drivers working for ride hailing apps such as Ola and Uber.

- The UN Broadband Commission for Sustainable Developmenthas released a report entitled 'Reimagining Global Health through Artificial Intelligence: The Roadmap to AI Maturity' which argues that while low- and middle-income countries (LMICs) may have the most to gain from AI to transform health systems, they may also have the most to lose because of systemic health issues with new advanced capabilities, emerging threats, disease, underserved populations, rapid urbanisation, and misinformation and disinformation.

- ITUs recently released a report Connecting Humanity - Assessing investment needs of connecting humanity to the Internet by 2030 argues that to connect the remaining billion people to the internet by 2030 would require around US$428 billion.

- The Broadband Commission for Digital Development released 'The State of Broadband 2020: Tackling Digital Inequalities, A Decade for Action' report that is a call world leaders and heads of industry to place universal broadband connectivity at the very forefront of global recovery and sustainable development efforts.

- GSMA has released The State of Mobile Internet Connectivity 2020, providing an overview of the trends in global connectivity to and progress made towards closing coverage and usage gaps and addressing key challenges. The report found that while the coverage gap – those living outside of areas covered by mobile broadband networks – continues to narrow, there is still a considerable usage gap which is now six times larger than the coverage gap.

- The World Intellectual Property Organization (WIPO) has launched the WIPO Lex-Judgments, a free database of leading judicial decisions related to intellectual property (IP) law from around the world.

- ITU has released the "Digital Skills Insights 2020" report discussing the types of skills that will be needed in the digital economy and future labour market, the new jobs and associated skills requirements, specific digital technologies and their impact on skills development, new skills required to manage data and information generated online and also explore gender and digital skills.

- Global Network Initiative has released a policy brief, "Content Regulation and Human Rights: Analysis and Recommendations" that analyses over 20 recently enacted or proposed content regulation initiatives from around the world and makes recommendations on how to develop laws and regulations that address harmful content and conduct online while preserving freedom of expression and privacy.

- Accessnow's"Rightscon Online 2020 Outcome Report"provides an overview of the prevalent human rights and technology landscape and highlights the achievements, learnings, and participation of the global community.

- Dvara Research has published a working paper "Effects of Mobile-Based Financial Services on Migrant Households' Remittances and Savings - A Case Study of Migrant Workers in Dundahera" that examines the access and usage gap in mobile-based financial services for migrant workers.

- The Freedom on the Net 2020: The Pandemic's Digital Shadow indicates that the internet freedom has declined for 10 straight years - contributing to a broader crisis for democracy around the world. From surveillance to arrests, governments are using the novel coronavirus as cover for a crackdown on digital liberty.

- APrIGF has published the APrIGF 2020 Synthesis Document: Internet Governance for Good: Norms, Standards and Mechanisms.

- UNCTAD's new study 'COVID-19 and e-Commerce Impact on Businesses and Policy Responses', highlights the impact of COVID-19 on digital economy, e-commerce especially in poorer nations of Africa and Asia. According to the study, there is a notable increase in digital financial services in the 23 nations surveyed, mostly least developed countries, yet, e-commerce businesses have been subject to challenges during the crisis, especially pertaining to disrupted supply chains, logistical problems due to restrictions on the movement of people, and high broadband costs. This was eased by some measures taken by the public and private sectors which made it possible for businesses and consumers to use e-commerce services.

- The OECD has published the 'Digital Economy Outlook' that highlights the impacts of COVID-19 on the digital divide between rich and poor countries.

- The 2020 Network Readiness Index titled 'Accelerating Digital Transformation in a post COVID-19 Global Economy' highlights Sweden and Denmark boast the highest rank at the global level while Chad, the Democratic Republic of the Congo (DRC), and Yemen have the lowest overall ranking. In the Asia-Pacific region, the highest ranked countries are Singapore (3), Australia (12), and South Korea (14). India is ranked at 88 while China is ranked at 40 position.

- The ITU's Measuring Digital Development: Facts and figures 2020reporthighlights persistent connectivity gaps in rural areas.

- A joint statement was sent out by Civil Society expressing concern over proposals by the UK government which would undermine encryption especially through its Online Harms Bill.

- The European Union Blockchain Observatory & Forum published its report on EU Blockchain Ecosystem Developments.

- MediaNama has released Tech Policy Review, India July -Sept 2020.

- Verisign has released the "Domain Names Industry brief Nov 2020" that highlights a growth of 0.2% in domain names in the third quarter as compared to the second quarter. The total TLD is 370.7 million and in terms of country code TLD to 160.6 million.
- The International Telecommunication Union (ITU) released the 2020 edition of 'Digital Skills Insights', a collection of articles addressing the impacts of digital transformation on capacity and skills development.
- GSMA published its annual 'Global Mobile Trends 2021' highlighting some of the implications of the pandemic on telecom operators.
- ITU has published a report "The Last-Mile Internet Connectivity Solutions Guide: Sustainable connectivity options for unconnected sites" which provides guidelines to help policymakers and professionals achieve appropriate last-mile connectivity solutions.
- The Alliance for Affordable Internet (A4AI), has launched itsthe 2020 edition of its Affordability Report that highlights the need for affordable Internet especially due to the pandemic and suggests three steps critical to achieve success as far as broadband plans are concerned: (a) open consultations, (b) setting clear targets, (b) and committed funding.
- G20 releases report Report on Digital Health Implementation Approach to Pandemic Management on digital health interventions for pandemic management.

■■■

**Published by CCAOI**
**Contributors:** Amrita Choudhury, Swati Shinde, Shalini Raghaviah
**Contact:** info@ccaoi.in