July 2022

THE TECHNOLOGY NEWSLETTER

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

INTRODUCTION

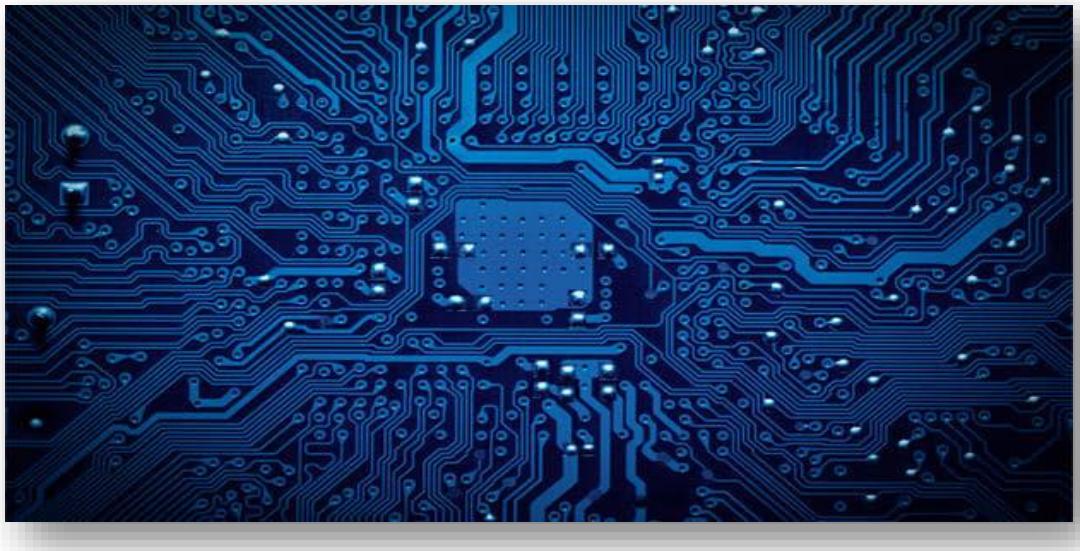
The Argus Technology Newsletter discusses recent developments in technological advances or milestones or events. As lawyers, we enjoy delving into the legal nuances and implications of technological changes and analysing their impact on our clients and their activities. It is said that law always lags behind technological advances and there could be some truth behind such statement, but there is no reason for lawyers to lag behind technological advances.

The Argus Technology Newsletter is not meant to be a substitute for your regular technology periodical. Instead, we hope and promise to offer a lawyer's insights into technological change and innovation.

Argus Partners has a developed a strong and a robust technology and data privacy practice, which spans transactional advisory, corporate and regulatory advisory as well as contentious matters and disputes. Whilst physically the attorneys are based out of our Mumbai, Delhi & Bangalore offices, the team is servicing clients across the globe on Indian legal issues in technology and data privacy.

Chinese cab hiring giant Didi fined $1.2 billion for data management policies resulting in risk to national security

Contributed by Aryan Mohindroo (Associate)



Didi Global Inc. ("**Didi**"), the Chinese cab hailing major, was fined more than eight billion yuan, pursuant to a year-long investigation of its data management policies. Along with Didi, Chinese regulators also fined Cheng Wei, Didi's Chairman, and Jean Liu, Didi's President, to the extent of one million yuan each. The penalties were levied by the Cyberspace Administration of China ("Administration"), which found Didi to be in violation of 3 (three) Chinese laws through actions which threatened the national security of China.

Didi had been one of the biggest targets of the Chinese regulators' widespread crackdown on various tech firms. The probe apparently found conclusive evidence that Didi was in violation of Chinese data protection regulations by illegally storing the personal information of more than 57,000,000 (fifty-seven million) drivers in plain text, instead of a more secure, encrypted format. It was further concluded by the Administration that Didi also analysed their passengers' details without their knowledge by accessing their photos and facial recognition information. As per the administration, the activities of Didi brought serious security risks to China's key information infrastructure and data security provisions. These violations are said to have been carried on for over 7 (seven) years beginning June, 2015 and included breaches of the Chinese Cybersecurity Law, Data Protection Law and Personal Information Law modelled on the EU GDPR law.

The fine imposed on Didi represents about 4.6% (four-point six percent) of Didi's revenue in 2021. As a result of the probe, Didi has been forced to delist from the New York Stock Exchange. This probe is a part of a series of crackdowns carried out by Chinese regulators on the country's tech firms, as a result of which a $2.75 bn fine has been imposed on Alibaba Group in 2021 for antitrust violations and a $527 mn fine on Chinese food delivery giant Meitun.

Compliance by big tech with Indonesia's new content law

Contributed by Anushkaa Shekhar (Associate)

Indonesia lacks a data protection regime but that hasn't stopped huge tech companies from establishing data centres and other facilities in the country, especially with the expanding number of Internet users expected to boost the economy in the coming years.

The Ministry of Communication and Informatics ("**MOCI**") of Indonesia issued Ministerial Regulation Number 5 ("**MR5**") on December 2, 2020 to regulate Electronic System Operators ("**ESO**") in the Private Sector. MR5 attracted immense criticism for being published without public consultation and for being a tool for censorship. Some of the provisions of MR5 are:

1. **Registration obligation for Private ESOs**

   MR5 requires companies classified as 'Private Electronic System Providers' to register with MOCI to continue operating in the country. Private ESOs are defined as individuals, businesses, or communities that operate an electronic system. They include:

   a. ESOs that are supervised by ministers or institutions in accordance with Indonesian laws and regulations.
   b. ESOs that have an online portal, site or application through internet to, inter alia:

      i. provide, manage and/or operate financial transaction services;
      ii. provide paid digital information or content to a user's device via a data network, either by downloading from a portal, email delivery, or another application;
      iii. process personal data for operational activity serving society in relation to electronic transactions.

   c. Entities that provide services or conduct business activity in Indonesian territory.
   d. Entities that offer their electronic systems in Indonesian territory.

Therefore, private ESOs such as e-commerce platforms, social media applications and game application operators are required to comply with the registration requirements under MR5.

2. Handling of Prohibited Electronic Information or Documents

In addition to the registration obligation, Private ESOs must also guarantee that their electronic systems do not include or assist the spread of unlawful electronic information or documents.

Prohibited electronic information or documents are those that:

a. violate existing rules and regulations; or
b. are upsetting to the public or threaten public order; or
c. provide ways or access to transmit illegal electronic information or documents.

Failing to comply with this provision could attract a ban by MOCI.

3. Access to Electronic Data for Government Authorities

MR5 allows Indonesian ministries, institutions, and law enforcement agencies to seek access to a private ESO's electronic system and data, and the private ESO is under an obligation to grant access upon receipt of a request from any competent government authority. Private ESOs are required to appoint at least one liaison officer who is based in Indonesia to handle requests for access from government officials.

Under MR5, the deadline to comply with the registration obligation was initially May 24, 2021. Despite receiving a backlash from human rights organizations for granting broad and unfettered powers to government officials to monitor online content, access user data, and penalise corporations that fail to comply, MR5 was further amended through Ministerial Regulation 10 ("**MR10**"), released on May 21, 2021. The amendment did not address any of the previously recognised concerns with MR5. Rather, MR10 simply added the requirement for private ESOs to register within six months after the launch of Indonesia's Online Single Submission system. MOCI later extended the deadline to July 20, 2022 for private ESOs to register themselves under MR5 and MR10.

This deadline was also met with widespread objection on the grounds that forced registration of private ESOs violates both Indonesia's constitution and international human rights responsibilities. It was also argued that the regulations will aggravate the already existing obstacles to freedom of opinion and expression in the country, as well as substantially restrict internet freedom.

Seeing no response from the government, many big techs including Meta, TikTok and Twitter applied for a licence from MOCI, immediately before the deadline. MOCI has already begun blocking access to various platforms that have not applied for registration, including PayPal, Steam and Yahoo. As a form of protest, residents and internet users have started circulating hashtags like "BlokirKominfo" (block Communication Ministry) on twitter.

Account Aggregator Framework and its growth in recent times

Contributed by Anurag Prasad (Associate)

Introduction:

An account aggregator ("**AA**") is non-banking financial company ("**NBFC**") which is licensed by the Reserve Bank of India ("**RBI**") to act as a consent manager for financial data on behalf of the customers of financial services. An AA, with the prior consent of the customer, collects data from financial information providers that hold an individual's personal financial data like banks ("**FIP**") and shares this data with financial information users that provide financial services to the individual ("**FIU**") in an encrypted format.

Industry Alliance of the Account Aggregator Ecosystem (Sahamati):

Sahamati (DigiSahamati Foundation) ("**Sahamati**"), is routinely in talks with more FIPs and FIUs to onboard them on the AA ecosystem. Sahamati is a not-for-profit private limited company under Section 8 of the Companies Act, 2013 set up as an industry alliance of the participants of the AA ecosystem, formed to promote and strengthen the AA ecosystem in India is working towards providing financial users, better control over their data and gain access to many innovative services and products.

How does the account aggregator framework empower a financial services customer?

AAs use technology to assist the customer securely transmit their data to financial institutions like banks, insurance agencies or mutual fund companies.

A customer can, with the help of an AA, use its financial data to access a vast array of financial services for its personal or business needs.

A flowchart of how the data sharing works in real time leveraging the AA framework is explained by Sahamati on its website, which is extracted below:

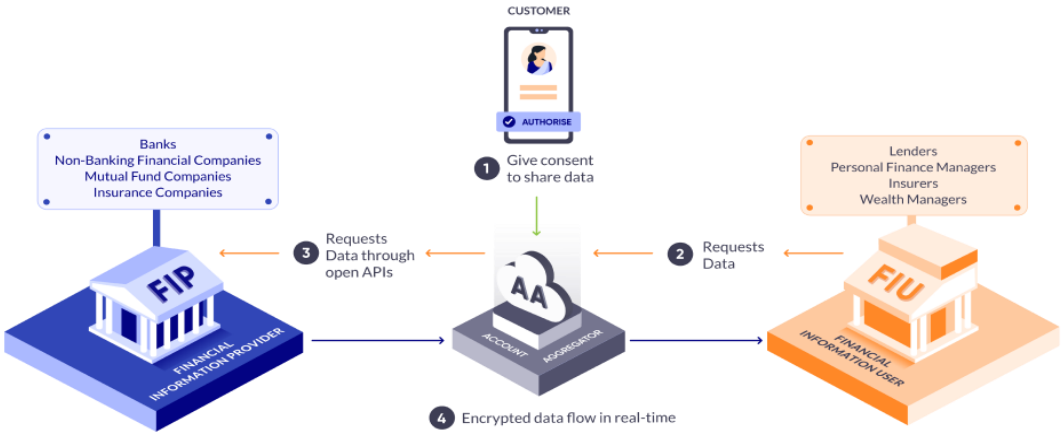


Image source: Sahamati[1]

Notable advantages of the AA framework:

1. The data set shared by the AAs ensures that a comprehensive financial profile of the customer is shared with the service provider on a real-time basis. This results in quicker processing of information by the service providers to allow fast access to credible customers.

2. Since the financial information is directly delivered from authorised accounts, the probability of data errors which happens due to manual provision of information by the customers is reduced significantly.

3. The AA framework incorporates privacy by design and empowers the customers to consent to and revoke the consent to share their financial information.

4. AAs keep the information encrypted at all times and ensure that no data is stored or processed by them.

Executive push and Increase in the participation in recent times:

The AA framework was introduced in September 2021, and was quickly adopted by leading private banks, NBFCs and insurance companies.

On July 7, 2022, the Ministry of Finance instructed all public sector banks ("**PSBs**") to onboard the AA framework by the end of July. As a result of this, recently, 8 (eight) PSBs viz., Canara Bank, Bank of India, Indian Bank, Punjab National Bank, Union Bank of India, State Bank of India, Bank of Maharashtra and UCO Bank have gone live on the AA ecosystem in some or the other capacity and other PSBs have also started testing the AA ecosystem.

[1]Image Copyright © 2022 - DigiSahamati Foundation

Guidelines on capturing consumer location by UPI application

Contributed by Rohan Mitra (Associate)

The National Payments Corporation of India ("**NPCI**") *vide* an operating circular published on July 5, 2022 ("**Circular**") has provided guidelines on capturing customer location on Unified Payments Interface ("**UPI**") applications.

UPI applications operate based on an Application Programming Interface ("**API**") framework, where geo tagging (location/ geocode) information of the payment is captured while initiating a transaction. These location details along with other relevant customer data need to be captured within the app providers system in an encrypted format. Since geo-tagging involves customer centric information and such data points are sensitive information, the relevant guidelines are necessary to be strictly followed by all UPI members.

The Circular provides the following guidelines:

1. UPI applications are only allowed to capture location/ geographic details with the consent of the customer/ individual, and the same cannot be made a mandatory feature.
2. If the customer had initially given consent to share their location with the UPI application while availing their services, the option for subsequently revoking such consent should also be provided. UPI services should be continued to be provided even if customer has revoked consent for sharing location/ geographical details.
3. In cases where consent has been given by the customer to capture location/ geographic details, the same should be correctly passed to UPI. Any incorrect details passed will attract strict action from the NPCI.
4. No UPI services shall be disabled or withheld from the customer if consent for sharing any location/geographic details has not been permitted.
5. These guidelines will be applicable where the customer (payer) is a person/ individual who is initiating the transaction and will be applicable to domestic UPI transactions only.

All UPI members are required to comply with the guidelines by December 1, 2022.

Delhi High Court refuses blanket injunction against GoDaddycom LLC from registering SNAPDEAL trademark

Contributed by Akshay Bhatia and Niharika Sharma (Associates)

The Delhi High Court ("**Court**") through an order dated July 13, 2022, refused to pass a blanket order restraining GoDaddycom LLC ("**GoDaddy**") and other Domain Name Registrars ("**DNRs**") from offering any domain name which incorporates Snapdeal Private Limited's ("**Snapdeal**") registered trademark 'SNAPDEAL'. The Court made it clear that a plaintiff ought to identify each infringing domain name against which relief is sought and that an overarching injunction order against DNRs, without identifying specific domain names, cannot be granted.

Background:

Snapdeal has filed a suit against GoDaddy and other DNRs seeking a permanent injunction restraining the DNRs from registering domain names that infringe its registered trademark. The Court, in an earlier order dated April 18, 2022, had held that an omnibus and global injunction cannot be granted restraining DNRs from offering any domain name with the name 'Snapdeal' in it. The Court had also held that 'Domain Name Registrars' are 'intermediaries' under Section 2(1)(w) of the Information Technology Act, 2000. We had covered the issue in detail in the April 2022 edition of our Technology Newsletter (here).

Now, during the hearing on July 13, 2022, the Court noted that while a suit cannot be continued in perpetuity qua the infringement of a particular mark, it would be cumbersome and expensive to expect a plaintiff to approach a court each time a domain name containing its trademark was registered. In response to this observation by the Court, GoDaddy submitted that it already has an internal 'Abuse Policy', that enables trademark owners to fill up a form to seek suspension/ locking of the domain name complained of.

Court's suggestions:

In the context of GoDaddy's submissions that an abuse policy already exists, the Court opined that the time has come for DNRs to create an independent and impartial mechanism, for e.g., an ombudsman, through which any trademark owner who has an objection to any registered domain name can approach the relevant DNR and seek cancellation/ transfer of the said domain name. In case the relief sought by the trademark owner, i.e., cancellation/ transfer is not sufficient, then the aggrieved trademark owner could avail remedies in accordance with

law. In the Court's opinion, such mechanism would involve an abuse policy, which would not merely deal with suspension/ locking of the domain names but should also be able to cancel/ transfer the infringing domain names. The Court also expressed its view that such abuse policy/ mechanism should be enforced by officials situated in India to ensure that in case the cancellation/ transfer is not permitted under the abuse policy/ mechanism, the trademark owner would be able to avail remedies before courts in India against the decision of the DNR.

To this end, the Court called upon GoDaddy to explore the possibility of a) setting up an independent and impartial mechanism to prevent the abuse of trademarks through registration of domain names; and b) amending its privacy features/ policy to make available the details of the registering person in respect of domain names on the 'Whois' database. The Court also issued a direction to the Department of Technology ("**DoT**") to clarify the manner in which DNRs who are offering services and earning revenue from India, despite being based out of other countries, may be made to obey orders passed by courts in India.

Conclusion:

The Court's observation that there is a pressing need for the establishment of an independent and impartial mechanism to prevent the infringement of trademarks through registration of domain names, is a welcome step. It provides an avenue for trademark owners to address their grievances directly with DNRs, in respect of infringing domain names infringing their trademarks, instead of having to approach a court of law each time an infringement is discovered. Currently, approaching a court of law is the only remedy available to a trademark owner to protect its trademark against such infringing domain names. This is an expensive and time-consuming process as lakhs of domain names are registered in respect of well-known trademarks. Further, the Court's view that the abuse policy should be implemented by DNRs through officials situated in India is also of note, as DNRs operate globally and typically do not have physical presence in each country they operate in. If the Court's suggestions were to be implemented, each DNR offering services in India would be required to have officials based in India. The Court has called upon GoDaddy and the DoT to submit their responses to these suggestions. Further developments in this ongoing litigation and implementation of the Court's suggestions in the future could go a long way in making expeditious and effective remedies available to a trademark holder in respect of infringing domain names as well as clarifying compliance obligations of DNRs in this regard.

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
knowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com

Contributing Partners:

Vinod Joseph, Partner
vinod.joseph@argus-p.com

Udit Mendiratta, Partner
udit.mendiratta@argus-p.com

MUMBAI
11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 6736 2222

DELHI
Express Building
9-10, Bahadurshah Zafar Marg
New Delhi 110002
T: +91 11 2370 1284/5/7

BENGALURU
68 Nandidurga Road
Jayamahal Extension
Bengaluru 560046
T: +91 80 46462300

KOLKATA
Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

www.argus-p.com I communications@argus-p.com