June 2021 | www.ifheindia.org/fol | Volume 3

ICFAI LAW SCHOOL HYDERABAD

CYBERNews

A Bi-monthly Newsletter of
The Centre of Excellence in Cyber Law and Data Protection

Upcoming Events

- Webinars
- Guest Lectures

Events Organized

- Webinars
- Guest Lectures

Rankings

- The ICFAI Law School, Hyderabad ranked 3rd Among TOP LEADING LAW SCHOOLS OF SUPER EXCELLENCE among Government and Private Law Schools in India by CSR-GHRDC – 2021
- The ICFAI Law School, Hyderabad ranked 1st Among Top Law Schools of Telangana among Government and Private Law Schools by CSR-GHRDC – 2021
- ICFAI Law School, Hyderabad ranked 1st among the top ten Law Schools in India according to The Academic Insights, 2020.
- ICFAI Law School, Hyderabad is ranked 3rd among top law schools. – India Today

Editorial Board

Students

Center Coordinator's Message

INDIA'S DATA PRIVACY LAWS AND START-UPS:

The vast number of the fast-growing start-ups in India make use of cloud computing services from the organizations like Amazon Web Services, Microsoft Azure, and others for data storage and processing. They depend on the cloud for hosting front-end and critical infrastructure, for compatibility in storing and processing the huge amount of data and reduce maintenance costs associated with available systems.

The criticism regarding small and medium scale start-ups for not having a full-fledged and robust cybersecurity environment isn't enough to fix the state of data protection among the ecosystem. The professionals, cyber security experts, and lawyers draw out the inferences that the Indian government's lackadaisical approach when it comes to protecting citizen data and privacy has been a major factor for companies refusing to follow basic disclosure practices in the event of leaks or breaches. If the tech start-ups continue to remain unchecked and unregulated without any imposition of penalties for leaking user data, then safeguarding sensitive data will inevitably transform in to a tremendous challenge.

The Information Technology Act serves as the only safeguard against data breaches with penalties and criminalization of companies which do not take prophylactic measures to protect user data. The IT Act was reinforced in 2011 with additional safeguards for "reasonable security practices and procedures" to be followed by companies that handle sensitive personal data (IT Rules, 2011). This has brought a new set of penalties and criminalization of companies found to violate the privacy of its customers but are not in synchronization with the norms incorporated in the GDPR.

There are shortcomings in the legislations as many companies strongly deny data leaks in public and even fail to bring the matter to the notice of government agencies. At present, businesses are expected to report all cyber security vulnerabilities and data breaches to the Computer Emergency Response Team (CERT-In), an arm of the IT ministry, but such notices are not mandatory. The Tech start-ups in India are told that they should choose ethics over profit, transparent public disclosure rather than covering up and protection of consumer data over their own benefit.

Recent Events

Conference on Data Privacy- A Cyber Colloquium on the 4- 5th June 2021.

In the globalized era of technological change, the individuals and Governments today feel that there is an increasing lack of control on data and data privacy. There is a need to respect privacy, safeguard the data of everyone and earn the trust of society at large.

Keeping in view the main objectives the ICFAI Law School, Icfai Foundation for Higher Education, Hyderabad has organized the two-day National Conference on Data Privacy- A Cyber Colloquium on the 4- 5th June 2021, under the auspices of Centre for Excellence in Cyber Law and Data Protection on the virtual platform.

The Inaugural session was graced by Director Sir, Prof. Dr. A.V. Narsimha Rao Icfai Law School, ICFAI Foundation for Higher Education, Hyderabad, Dr. Pavan Duggal, Advocate, Supreme Court of India Chairman, International Commission on Cyber Security Law and Guest of Honour, Mr. U. Ram Mohan, SP, Andhra Pradesh.

The inaugural ceremony began with spiritual invocation followed by a welcome note by Dr. Md Akbar Khan, the coordinator for the program. He introduced the event organized under the auspices of Centre for Excellence in Cyber Law and Data Protection and four technical sessions to be followed with themes like Phylogenetic Facets of IT Legislation, Data Breach and Risk Analysis, Media Intrusions and the Privacy Challenges and Career Planning and Data Protection within a span of two days and emphasized that they are absolutely going to be industrially benefitting and academically rewarding.

Prof. Dr. A.V. Narsimha Rao Icfai Law School, ICFAI Foundation for Higher Education, Hyderabad addressed the audience and spoke on the significance of Right to privacy under Art 21 of the India Constitution and also stressed that data privacy plays a challenging role in the absence of a proper legal framework and culprits misusing the stored information through electronic devices and he suggested that necessary safety measures to be adopted in order to avoid violation or breach of privacy.

Dr. Pavan Duggal, as an expert on cyber Law Issues addressed to the virtual audience emphasizing the need to understand the nuances of privacy in India and the world at large and the need for a legislation in the said area. Privacy was of vital importance in the areas of Health, social media and other areas and he also spoke at length at its misuse in certain areas. He also stressed the need for individuals to also understand the privacy challenges in the Indian context and correlated the same to the Data protection bill 2019 in India and the world at large.

The Guest of honour for the inaugural session Mr. U. Rammohan, SP, spoke on the need to look at the way that cyber-crimes have been on the rise during the pandemic. He spoke at length on how cyber criminals have outsmarted the systems and the cyber security measures that have been put in place at various levels by organizations and individuals. He also stated that even organization like SCADA is also vulnerable.

The inaugural ceremony was gracefully concluded with a vote of thanks presented by Mr. Rakesh Suryadevara the co-coordinator for the program.

The first technical session dealt with "A Phylogenetic Facets of IT Legislation", chaired by Dr. Subhajit Basu, FRSA, Editor in Chief, IRLCT, University of Leeds, U.K.,

The second technical session, Data Breach and Risk Analysis was chaired by Dr. Harold D Costa, President Cyber Security Corporation and the keynote speaker for the same was our Director sir, ICFAI, Law School, IFHE, Hyderabad.

The third technical session was "Media Intrusions and the Privacy Challenges – Legal Dynamics", chaired by Mr. Ashok Ram Kumar, Senior Attorney, Adjunct Faculty ICFAI Law School and the keynote speaker was Mr. P. J. Blount, Adjunct Professor, Mississippi School of Law, USA.

The fourth one was "Career Planning and Data Protection" chaired by Dr. Ranjit Oomen Abraham, Assistant Professor, the Tamil Nadu Dr. Ambedkar Law University and the key note speaker was Mr. Abhishek Mitra, CEO and Founder, Indian Cyber Security Solutions.

The co-chairs were Dr. Md Akbar Khan, Dr. Jayanth Reddy, Mr. Rakesh Suryadevara and Dr. Vinay Sharma.

Valedictory session was graced by the chief guest Mr. Mukesh Choudhary, Founder & CEO of Cyberops Infosec. He is a Cyber Crime Consultant and Information Security Professional.

Also best papers were awarded with Cash Prizes.

Third Best Paper Rs.1000/- : DATA, LAWFUL PURPOSE, AND INFORMED CONSENT: A COMPARITIVE LAW ANALYSIS OF DIFFERENT LEGISLATIONS.

Author: Ms. Sumedha Ganjoo, PhD Scholar, Bennett University;

Co-Author: Dr. Garima Tiwari, Asst Prof, Bennett University.

Second Best Paper: Rs.2000/- :

The Data Protection Laws and The Right to be forgotten:

Analyzing the Indian Legal Perspective.

Author: Ms. Neha Purohit , Asst Prof, RNB Global University.

Co-Author: Mr. Jai Prakash, Advocate, Supreme Court of India.

First Best Paper: Rs. 3000/- : Post Schrems II - Impact on lawful sharing of data for health research: Lessons for India.

Author: Ms. Akanksha Bisoyi, Student, Master in International Law, Graduate Institute of International and Development Studies, Geneva.

Case Law / News

Delhi High Court Judgement on CCI Inquiry into Whats app's new data privacy policy in India

The issue as to whether the sharing of the information available with WhatsApp with Facebook violates the right of privacy of the users protected under Article 21 of the Constitution of India, and as to whether the petitioner(s) are under any legal obligation to provide an 'opt-out' facility to the users of WhatsApp, are issues that are pending adjudication before the Constitutional Court, and especially the Constitutional Bench of the Supreme Court, and , therefore, it was not open for CCI to consider the same issues in exercise of its *suo moto* powers under the Competition Act, 2002 (the Act) .

Judicial discipline would demand that CCI ought to have refrained from adjudicating on the said issues till the same are pronounced upon by the Supreme Court and the Delhi High Court in the above-referred proceedings.

The High Court after hearing the rival contentions as above has decided as under

- Appreciated the CCI's *prima facie view* that WhatsApp is dominant in the relevant market for Over-the-Top (OTT) messaging apps through smartphones in India; due to lack of/restricted interoperability between platforms, the users may find it difficult to switchover to other applications except at a significant loss; there is opacity, vagueness, open-endedness and incomplete disclosures in the 2021 Update on vital information categories; concentration of data in WhatsApp and Facebook itself may raise competition concerns; data-sharing amounts to **degradation of non-price parameters of competition.**
- that the **scope of inquiry before the CCI** is not confined only to the issues raised before the Supreme Court or before this Court, but is **much vaster in nature.**
- Held that the issue as to whether the 2016 Update/2021 Update announced by WhatsApp in any manner infringes upon the Right of Privacy of the users guaranteed under Article 21 of the Constitution of India is pending adjudication before the Supreme Court and this Court.
- Rejected the contention of Facebook that its impleadment in the investigation was unwarranted.

AIR INDIA DATA BREACH

In a major cyber-attack that has hit global airlines, including Air India, data of 45 lakh users have been compromised. Air India informed that its SITA PSS server, which is responsible for storing and processing personal information of fliers, was subject to a cyber-security attack. The resultant data breach involved personal data registered between August 26, 2011 and February 20, 2021. In this attack, details like name,

date of birth, contact information, passport details, ticket information, Star Alliance and Air India frequent flyer data as well as credit card data were leaked.

In regard to credit cards' data, Air India clarified that CVV/CVC numbers are not held by SITA.It said that the identity of its affected passengers was provided to it by SITA on March 25 and April 5 only.Air India along with the service provider is carrying out risk assessment and would further update as and when it becomes available, it said. The airline said it has taken following steps after the data security incident: Secured the compromised servers, engaged external specialists of data security incidents, notified and in talk with the credit card issuers and reset the passwords of Air India frequent flyer programme.

The breach raises fresh concerns after allegations earlier this year that Chinese intrusions may have affected operations at a key stock exchange and disrupted power supply in Mumbai, the country's commercial hub. Cyber-attacks have become a growing threat in recent months with hacker groups targeting research institutions in Japan to American government agencies, which include an attack mainly on health care data, data of Government agencies and business.

RANSOM WARE ATTACKS: A SHIFT IN PRIORITIES FOR GOVERNMENTS

Number of organizations impacted by ransom ware globally has more than doubled in the first half of 2021 compared with 2020.The healthcare and utilities sectors are the most targeted sectors since the beginning of April 2021.Organizations in Asia Pacific are targeted more than any other region and ransom ware attacks had seen a 57% increase in the number of attacks since the beginning of 2021 amid the disclosure of the Microsoft Exchange vulnerabilities.

Most recently, Colonial Pipeline, a major US fuel company, was the victim of such an attack But after the ransom ware group Dark side attacked the East Coast oil and gas supplier Colonial Pipeline, which led to an 11-day shut-down and gas shortages in the Eastern US, it appears that the federal government is no longer satisfied with private industry's lagging cyber security protections. Already, President Joe Biden has signed an Executive Order to place new restrictions on software companies that sell their products to the federal government. Those rules were reportedly refined after the Colonial Pipeline attack, and are expected to become an industry norm as more technology companies vie to include the government as a major customer.

NEW LAWS FOR REVENGE PORN IN INDIA

The Ministry of Women and Child Development is seeking to make changes in the laws to deal with cybercrimes against women, there will also be a special focus on revenge porn, and plugging existing loopholes in the laws on the subject.

Revenge porn is when private, intimate images, often of a sexual nature, are uploaded or shared without the person's consent. The upload/sharing is often by former partners, jilted lovers and the like, for the purpose of seeking revenge and as per the Laws in India revenge porn is currently punishable.

Even without the specific laws, revenge porn is a crime, punishable with between 3-7 years imprisonment and a fine of upto Rs. 10 lakhs, under various sections of the Information Technology Act, 2000 and the Indian Penal Code, 1860.

Steps are needed to ensure speedy removal of such content. Under the IT Act, removal by a website within 36 hours is ensured only when there is a court/ govt order. This should be removed for specific crimes, such as revenge porn. Also, judicial processes need to be expedited, such as through establishment of dedicated Courts and prescribing timelines. While laws protecting women are required, men are equally susceptible to a crime like revenge porn. It should be ensured that male victims also have adequate protection under the law.

One problem is that most of these laws come into play after the upload is done. By then most of the damage is already done, with sharing and re-uploads of the content happening at a rapid pace, whether by the viewers or on multiple websites.

To control dissemination of such content, the recent MEITY order directing ISPs to implement Internet Watch Foundation resources to prevent the distribution and transmission of child sexual abuse material needs to be extended to revenge porn material.

Research needs to be directed towards developing technology that can help with effectively preventing the spread of such material. Also, imposing greater responsibility on intermediaries should be considered.