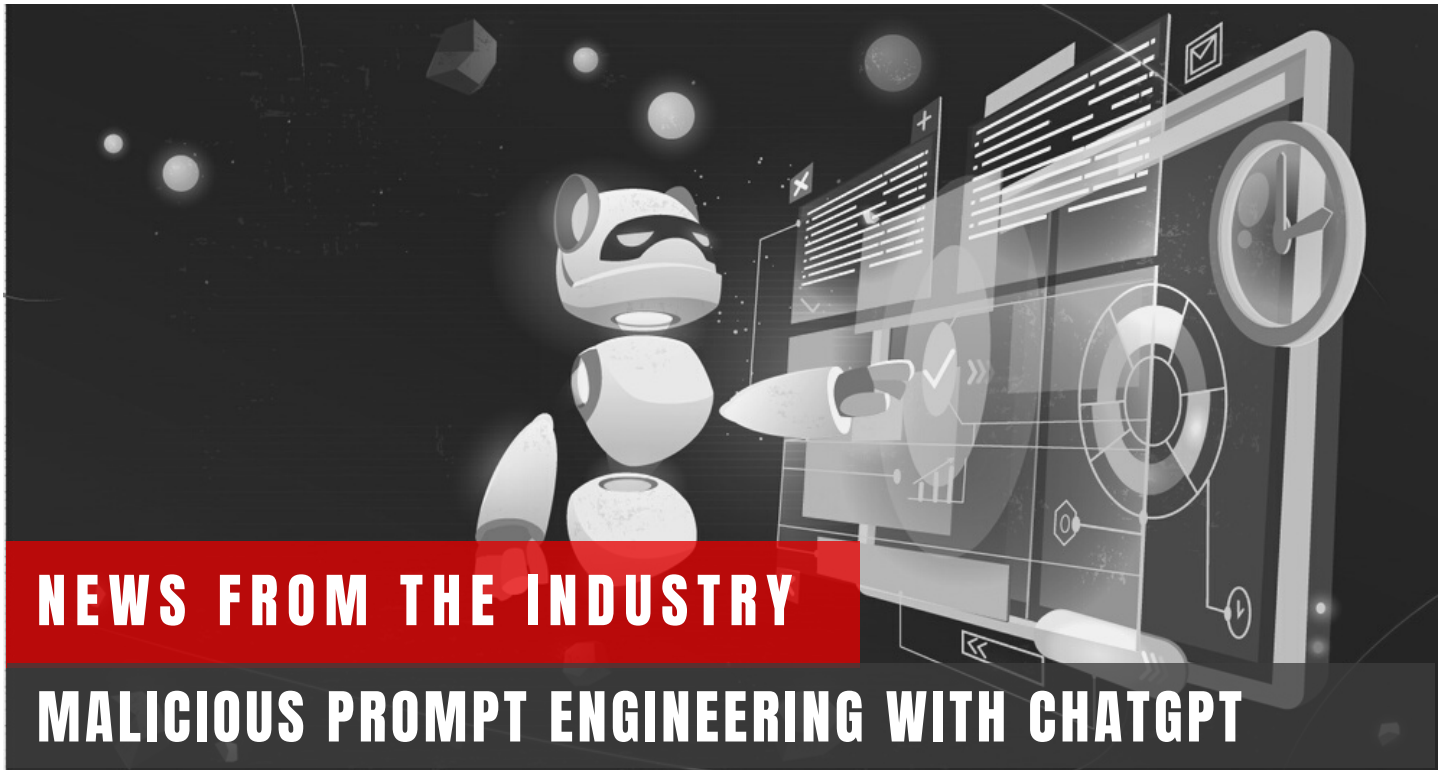
INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet



NEWS FROM THE INDUSTRY

MALICIOUS PROMPT ENGINEERING WITH CHATGPT

OpenAI's chatbot, ChatGPT, has been a major breakthrough in technology, with tasks requested through prompts. However, the emergence of malicious prompt engineering has raised concerns. This process is similar to social engineering and highlights the potential for abuse. Most of the information about prompt engineering on ChatGPT is available on Twitter, where concrete examples have been provided. The advantage of making ChatGPT accessible to the public is that it demonstrates the potential for abuse and spurs the development of better filters to prevent unauthorized use in future. Despite these efforts, attackers will likely switch to new vulnerabilities as defenders close existing ones.

The researchers conducted a study in which a malicious prompt was used to create a phishing email with GDPR as its basis. The prompt asked the target to upload content to a new location that had allegedly been deleted in order to comply with GDPR requirements.

IN THIS NEWSLETTER

Further prompts were used to create an email thread supporting the phishing request, resulting in a convincing phish free of the usual typos and grammar mistakes. Malicious prompts have also been used to generate fake news and harass individuals. It is important to note that any investigation into the application of prompt engineering is only relevant at the time of the investigation. AI systems will continue to engage in the cybersecurity leapfrog process, with attackers switching to new vulnerabilities as defenders close existing ones. Despite this challenge, the development of better filters will make unauthorized use more difficult in the future, providing a safer and more secure online environment.

SUPPLY CHAIN ATTACKS CAUSED MORE DATA COMPROMISES THAN MALWARE

The Identity Theft Resource Center, an organization based in the United States of America, reported that in the first half of 2022, there were fewer data breaches which can be attributed, in part, to the fact that cybercriminals based in Russia were occupied with the conflict in Ukraine and the unstable state of the cryptocurrency market. However, in the second half of the year, data breaches increased with a total of 422 million people being impacted, representing a 41.5% increase from the previous year.

This rise was largely due to the personal information of 221 million Twitter users being available on illegal identity marketplaces. Cyberattacks continue to be the primary cause of data breaches and in 2022, supply chain attacks surpassed breaches caused by malware. While malware is often the source behind cyberattacks, in 2022, the number of supply chain attacks was 40% higher than malware-related breaches.

INDIA'S EDUCATION MINISTRY EXPOSED DATA THROUGH UNSECURED SERVER

A security lapse in the Digital Infrastructure for Knowledge Sharing (Diksha) application operated by India's Ministry of Education has exposed the personally identifying information of millions of students and teachers. As per reports, the data was stored on an unsecured cloud server, making it accessible to hackers and scammers. Files on the server contained names, phone numbers, and email addresses of more than 1 million teachers and nearly 600,000 students. The UK-based security researcher who discovered the exposure in June reached out to Diksha's support email but received no response. The researcher believes that the data has been accessed and downloaded by others.

DUOLINGO INVESTIGATING DARK WEB POST OFFERING DATA FROM 2.6 MILLION ACCOUNTS

Duolingo, a popular language learning platform, is investigating a dark web post that claims to have information from 2.6 million user accounts. The company has stated that no data breach or hack has occurred and that the records were obtained through data scraping public profile information. This process involves a computer programme extracting data from the output of another programme and saving it in a local file for manipulation and analysis. The hacker provided a sample of 1,000 accounts. The scraping of social media platforms and websites is a significant issue for many of the largest tech companies, with web scraping increasing 240% YoY mostly due to use of bots by cybercriminals.

THIRD-PARTY RISK CONTRIBUTES TO HEALTHCARE DATA BREACHES

Healthcare data breaches have significantly increased between 2018-2021. A large portion of these breaches were caused by third party service providers at healthcare facilities. Data shows that during the first half of 2022, 72% of healthcare data breaches were a result of healthcare providers. These incidents demonstrate the difficulties businesses face, in protecting their valuable data. Cybersecurity risks from third parties are becoming a common and damaging problem. A report from CrowdStrike, an American cybersecurity technology company based in Austin, showed that in 2021, 45% of organizations reported at least one incident of a software supply chain attack. Furthermore, the report showed that the number of supply chain attacks is surging by 430%. In a recent survey among cybersecurity professionals, 64% of the participants stated that they would be unable to stop an attack from a compromised software supplier. Also, 71% of the organizations reported experiencing data loss or compromise of assets due to software supply chain attacks. To sustain resilience against increasing cyber threats, in healthcare, informed relationships with third parties and stronger internal measures are crucial.

OPENEMR, A HEALTHCARE SOFTWARE VULNERABLE TO REMOTE ATTACKS

OpenEMR, an open-source electronic health records software, has been found to have three security vulnerabilities by security researchers at SonarSource, a company that provides open source solutions for software quality and security. The company's static application security testing engine discovered that two of the vulnerabilities could lead to unauthenticated remote code execution. The third vulnerability allowed attackers to steal user data. SonarSource reported the issues to the OpenEMR maintainers on October 24, 2022, and a patch was released seven days later. The researchers at Sonar advise users of OpenEMR to update to the fixed version 7.0.0. This comes almost five years after researchers at Project Insecurity discovered over 20 flaws (now fixed) in OpenEMR.

1.7TB OF DATA STOLEN FROM AN ISRAELI DIGITAL INTELLIGENCE COMPANY; LEAKED ONLINE

Cellebrite, a prominent Israeli company that specializes in mobile forensics and works with law enforcement and intelligence agencies across the world, was recently targeted by activists and whistle-blowers. The reason being, the data of the company was leaked online by the Enlace Hactivist collective. One of its main services, known as the Universal Forensics Extraction Device, is used by law enforcement agencies to extract data from mobile devices. Hacktivists claim that this tool has been utilized, in the past, against journalists, activists and dissidents globally. There have been numerous reports that suggest that the government has used this technology to spy on citizens and journalists, violating human rights. The hacktivists have expressed their disappointment in Cellebrite for not conducting due diligence and for violating human rights, leading to data breach.

LACK OF QUALIFIED PEOPLE FOR RISK MITIGATIONS AND LAW COMPLIANCE IN ORGANIZATIONS

A new report by the international professional association focused on IT governance, Information Systems Audit and Control Association (ISACA) shows that there is a shortage of qualified people for risk mitigation and data privacy compliance, as organizations struggle with understaffed technical privacy and legal/compliance teams and skills gaps. This shortage can result in non-compliance with privacy laws, like the California Consumer Privacy Act (CCPA), which can be costly. According to the survey, around 25% of data privacy professionals work with the finance department but that number may need to increase as CFOs can play a key role in procurement. Meanwhile, the global cybersecurity market is expected to reach $403 billion by 2027, but a lack of funding for privacy budgets and clarity on roles and responsibilities is a concern for many organizations. Privacy and security should both be prioritized, as digital trust, of which privacy is a key component, becomes a priority for boards and the C-suite.

CENTRAL GOVERNMENT ORGANISES SYMPOSIUM FOR FINANCIAL SECTOR CYBERSECURITY CONCERNS

The Department of Financial Services, under the Ministry of Finance, Government of India, held a symposium titled Financial Services Cyber Security (FINSCY). The symposium provided an opportunity to senior officers from government agencies and financial sector regulators, banks, insurance companies and finance institutes to share their ideas, practices, and concerns on cyber security measures currently in place. They further discussed the readiness for India’s financial sector from cyber threats and the provisions for the draft Digital Personal Data Protection Bill, 2022.

US SCIENTISTS TO STUDY CYBER PSYCHOLOGY TO AVERT CYBER ATTACKS

Scientists at Intelligence Advanced Research Projects Activity (IARPA), Bethesda, United States of America, are investigating the use of psychology to combat cyberattacks. Their objective is to design systems that take into account human limitations, such as biases in decision-making, to prevent or delay hackers' actions. The increasing demand for technology that automates defence and detection tasks is due to the global shortage of cybersecurity talent. A number of technology companies are already offering products that incorporate findings from cyber psychology.

This research is a critical step in addressing the current shortfall of cybersecurity resources and effectively preventing cyber incidents. By incorporating human behaviours into the design of these systems, the aim is to make them more effective and responsive to the changing landscape of cyber threats.

DIGITAL DATA PRIVACY DAY

Data Privacy Day, also known as Data Protection Day, is celebrated annually on January 28 to raise awareness about the importance of protecting personal information and promoting data privacy. The day has been recognized globally to commemorate the signing of Convention 108, the first legally binding international treaty on data protection in 1981.

The world has become increasingly digital, and with the rise of technology, the amount of personal data being collected, stored, and shared has grown at an exponential rate. As a result, the protection of personal information has become a critical issue, and it is imperative that individuals understand the importance of safeguarding their data.

Data Privacy Day serves as a reminder for individuals to be vigilant about the information they share online and to take steps to protect their personal data. This can be done by reviewing privacy policies, securing online accounts with strong passwords and being cautious of suspicious emails and links. Individuals must play their part in protecting their personal information. Here are some best practices that individuals can follow to secure their personal data:

- Use strong passwords: Create strong and unique passwords for all online accounts and regularly change them.
- Be cautious of suspicious emails and links: Do not click on emails or links from unknown sources, as they may contain malware or phishing links.
- Review privacy policies: Before sharing personal information, review the privacy policy of the website or app to understand how your data will be used.
- Enable two-factor authentication: Use two-factor authentication for all online accounts to add an extra layer of security.

By following best practices and implementing strong security measures, we can create a safer and more secure digital world. With the increasing use of technology, it is essential that everyone takes the necessary steps to ensure the safety of personal data and promote a safer and more secure digital world.

OUR CONSULTATIONS

Consultation on Data Encryption and Traceability

India Future Foundation (IFF) organized a virtual consultation on 'Data Encryption and Traceability.' The Ministry of Electronics and Information Technology (MeitY) recently proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The Bill highlights continued engagement of tech platforms with the regulatory bodies in India, to ensure a balance between transparency, freedom of expression, and privacy.

There have been debates among policy experts and the social media intermediaries on the issue of encryption and traceability. With regard to this view, IFF hosted a virtual consultation on Data Encryption and Traceability to get the view of wide array of experts from academia, civil society, law enforcement, law and technology on the ongoing issue and possible alternatives for data traceability.

The event took place virtually on Microsoft Teams on January 13th, 2023 between 11 am to 1 pm. The speakers provided insights and opinions on various provisions of the Bill including future of end-to-end encryption, need for regulations, data traceability and mass surveillance, national security, grievance redressal mechanism, possible alternatives, traceability and the Right to Privacy.

Speakers at the consultation included : Col. (Retd) Debashish Bose, Senior Defence Specialist (Cyber) National Security Council Secretariat; Cdr (Retd) Sandeep Padam, Sr Director IT, Lowe's India; Dr Subi Chaturvedi, Chief Corporate Affairs & Public Policy Officer, InMobi; Ms Shweta Venkatesan, Legal Associate, Koan Advisory Group; Mr Salil Mittal, Lead Cyber Security - Emerging Technologies, Jio; Ms Surbhi Chakraborthy, Research Assistant, United Service Institution of India; Ms Lalantika, Legal Analyst, Koan Advisory Group and Mr Kanishk Gaur, Founder, India Future Foundation. The event was moderated by Mr Pankaj Toppo – Head – Policy Programmes and Research, India Future Foundation and Ms Manmeet Randhawa, Head Corporate Communications & Strategic Alliances, India Future Foundation.

OUR CONSULTATIONS

Consultation on the Impact of Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2021 with regard to Online Gaming Regulations

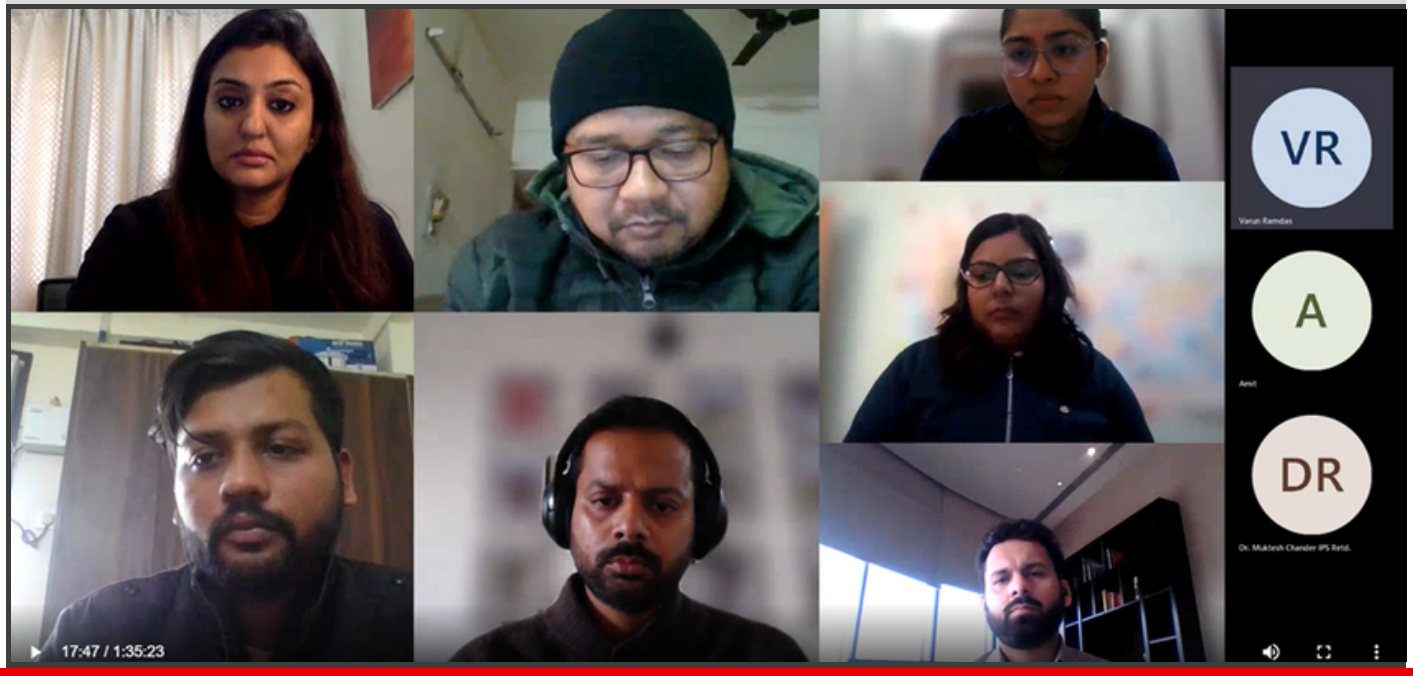
India Future Foundation (IFF) organized a virtual consultation on the impact of draft rules related to online gaming. The Ministry of Electronics and Information Technology (MeitY) recently proposed amendments to the Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

This Bill is a noble step towards providing a framework for regulations and facilitating the growth of online games. In order to understand and discuss on the scope of the provisions of this draft Bill, experts from various fields including policy, finance, law, cybercrime and technology were invited.

The experts provided their insights on various topics including composition of self-regulatory body (SRBs), OGI game registrations, due diligence & KYC, the need for having a central regulation for OGIs, definition of "online games", certification of online games, grievance redressal mechanism and so on.

The consultation was held virtually on Microsoft Teams on January 14, 2023 between 4 pm to 6 pm.

The speakers at the event included Dr Shruti Mantri, Associate Director, Indian School of Business, Dr Muktesh Chander, former Special Commissioner, Delhi Police and DGP Goa; Dr Subi Chaturvedi, Chief Corporate Affairs & Policy Officer, InMobi; Mr Varun Ramdas; Senior Associate, Koan Advisory Group, Mr Priyesh Mishra, Senior Associate, Koan Advisory Group; Dr Pawan Duggal, Chairman, International Commission on Cyber Security Law; Mr Amit Dubey, Co-Founder, India Future Foundation and Mr Kanishk Gaur, Founder, India Future Foundation. The event was moderated by Ms Manmeet Randhawa, Head – Corporate Communications & Strategic Alliances, India Future Foundation and Mr Pankaj Anup Toppo, Head – Policy Programmes and Research, India Future Foundation.

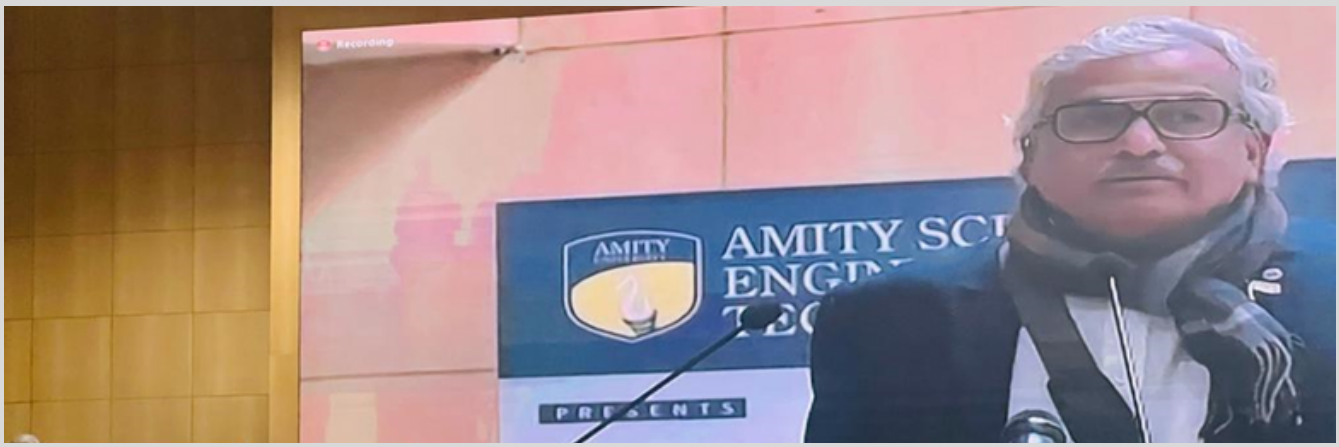


PANEL DISCUSSIONS

Workshop on Post Pandemic: Delivering Technology Outcomes as a Service at Confederation of Indian Industries Facilitated by Hewlett Packard Enterprise

Confederation of Indian Industry (CII) facilitated a workshop on January 30, 2023 on "Post Pandemic: Delivering Technology Outcomes as a Service" in association with Hewlett Packard Enterprise (HPE). Ms Manmeet Randhawa, Head – Corporate Communications & Strategic Alliances, India Future Foundation was invited as a panelist for the discussion and she shared her views about the need for mindset change and understanding sustainability as well as awareness required in adopting Infrastructure as a Service (IaaS) for the public sector and MSMEs. The discussion explored the changing Information and Communications Technology (ICT) infrastructure in the states of Haryana and Punjab. The workshop provided perspective on initiatives taken by the government and the value that ICT Infrastructure as a Service (IaaS) brings to public sector organizations.

Plenary Session on "ACADEMIA-INDUSTRY LINKAGE: A NECESSITY FOR CREATING NATIONAL ECOSYSTEM."



Amity School of Engineering & Technology, AUUP, Noida organized a CONFLUENCE with the Department of Computer Science & Engineering and Corporate Resource Centre. The CONFLUENCE was organized on 'Academia-Industry Linkage: A Necessity for Creating National Ecosystem.' The agenda of the event was to connect the academia with the corporate sector for sustained economic growth. The event was attended by experts from the corporate sector, cyber security and academia. Mr Amit Dubey, Co-Founder, India Future Foundation and Col (Retd) Sunil Kapila, Chief Technology Officer, Athenian Tech were invited as a panellist at the event.

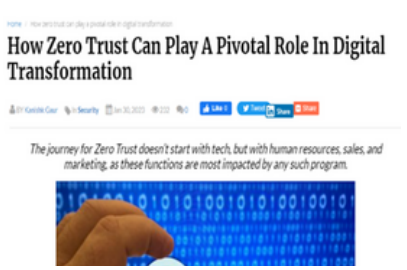
IFF IN THE MEDIA


Opinion: Why Cyber Attack on India has Civilian Casualty in Era of Hybrid Warfare?

There is an immediate need to modernise Military Doctrine to include Cyber as a key component of warfare. There is a need to further invest resources and talent to modernise India's Cyber Command, Cert Operations, Critical information Infrastructure organisation, and implementation of the National Security Operation Centre, which needs to be manned and run by Trusted Indian System Integrators.

ETGovernment • Updated: January 15, 2023, 23:43 IST

Kanishk Gaur, Founder, IFF shares his views on casualty on civilians in the era of hybrid war in The Economic Times.


How Zero Trust Can Play A Pivotal Role In Digital Transformation

The journey for Zero Trust doesn't start with tech, but with human resources, sales, and marketing, as these functions are most impacted by any such program.

Kanishk Gaur, Founder, IFF writes about Zero Trust's role in digital transformation in CIO&Leader.


The Need To Build Digital Culture In A Cost-Conscious World

In the current economic climate, organizations are looking for ways to cut costs and manage expenses more effectively. One way to do this is by building a digital culture within the organization.

Kanishk Gaur, Founder, IFF, shares his insights on the need to build digital culture in organizations in CIO&Leader.

Amit Dubey, Co Founder, IFF in a panel discussion on the Zee Business about OpenAI's chatbot, ChatGPT.

Kanishk Gaur, Founder, IFF in conversation about Gautam Adani in Glance Magazine.

INDIA FUTURE
FOUNDATION

Contact Us

+91-1244045954, +91-9312580816

Building no. 2731 EP, Sector 57,
Golf Course Ext. Road, Gurugram,
Haryana, India – 122003

helpline@indiafuturefoundation.com

www.indiafuturefoundation.com