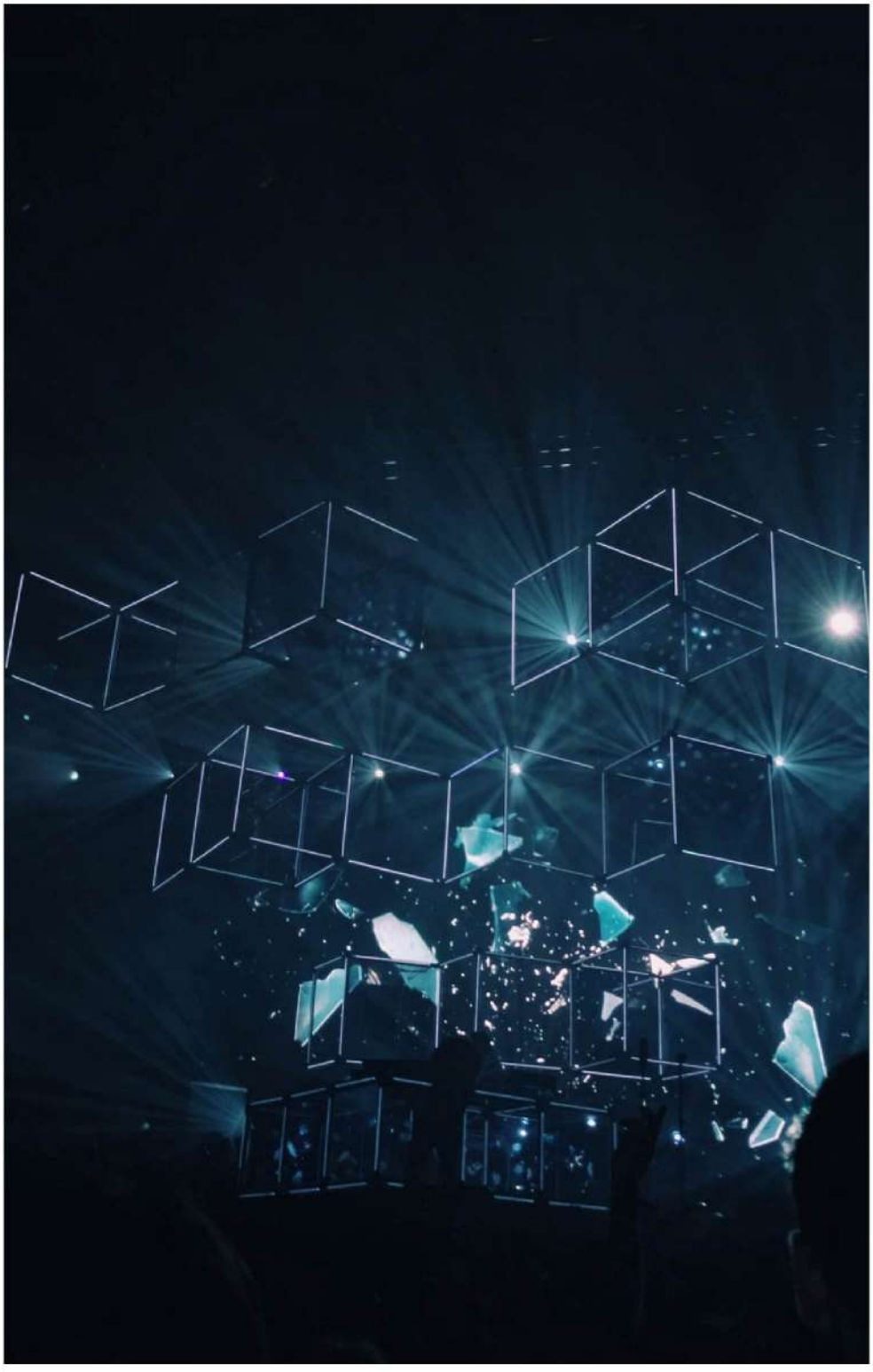
CyberPeace | Foundation

Data Privacy and Protection
The Indian Perspective



WHITE PAPER

Contents

I. Introduction

A. Globalisation - The Internet and tech gadgets have brought the world closer than ever, globalisation resulted in various global tech companies that are now tech giants, operating in India and providing their services and employment opportunities. The outsourcing of various jobs to India led to mass skill development which is thus aiding Indians in being self-sufficient in the current times.

B. Global and Indian Internet Penetration Index - The evolution of the digital age has resulted in a spike in Internet Penetration, since the advent of ARPANET, the influence of the internet has increased gradually but with booms like WWW, the penetration was increased exponentially, as of 2022 the global internet penetration index stands at 69% with India at 41%. [1]

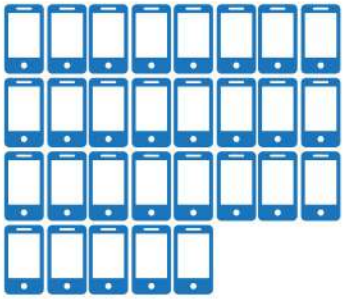
C. Tech Advancements and Comparison - The world has been witnessing advancement in science and technology since the last century, what started as a mechanical age has now turned into the digital age, earlier we had wrist watches now we have smart watches, chauffeur-driven cars have turned into auto drive cars, Telegram and letters have turned into emails, massive sized computers have turned into palm-sized smartphones thus signifying how we have transitioned from the analogue age to the digital age.

D. 4G Jio boom - In 2016 Reliance telecom launched the Jio network, this was the first affordable and high-speed 4G network available to the Indian consumer. The SIMs were provided for free and a trial connection of 6 months was given to the customer. This stint in the telecom market resulted in a reduction in data and calling prices by all telecom companies and the Indian consumer had access to high-speed networks even from the remotest part of the country.

E. Advent of 5G - The Indian consumer in major metropolitan and tier 1 cities can now avail of the 5G networks. All major telecommunication service providers like Jio & Airtel have started their services, and government-based BSNL is expected to launch its 5G services by 2023 August. This boom right after the pandemic and increased internet penetration will result in an increased engagement of Indian netizens in cyberspace.

F. Covid-19 Influence on Internet Penetration - After the boom of the 4G jio network, the pandemic accelerated the reach and internet penetration among the rural population, thus the pandemic was responsible to bring a majority of the population into the digital sphere as in today's time villages also have WIFI and 4G connectivity.

G. Use of Data by Govt & Corporates - The primary fruits of the digital age are automation and connectivity in all aspects of day-to-day tasks. In this spectrum Data, privacy and protection play a vital role in the digital world because every action in cyberspace leaves a digital footprint that is permanent. This is in turn data, which is provided by the user and utilised and processed by the service providers and the Govt. Data is the primary form of information in today's time and its protection and privacy are of paramount importance.



at the start of 2022

1.14 Billion

cellular mobile connections

between 2021 and 2022

34 million

(+3.1 Percent)

97%

of data breach incidents take place due to human error

81.3%

of the total population

H. <u>Data Usage Figures</u> - Data from GSMA Intelligence shows that there were 1.14 billion cellular mobile connections in India at the start of 2022. GSMA Intelligence's numbers indicate that mobile connections in India were equivalent to 81.3 percent of the total population in January 2022. The number of mobile connections in India increased by 34 million (+3.1 percent) between 2021 and 2022. The major issue at hand is the involuntary ignorance and unawareness on part of the people, data in itself is an essential part of our life, and can be used to do goods and harms of massive magnitudes. 97% of data breach incidents take place due to human error, thus making it clear that machines and devices are not responsible for cyber-attacks, instead, these devices and gadgets are mediums for such attacks and crimes.

I. <u>Global Data Protection Laws</u> - More than 120 countries have legislation to secure the Protection and Privacy of Data

1. EU's General Data Protection Regulation (GDPR), was implemented in May 2018.
2. he United States has a mix of laws like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, which aim to protect the data of all Americans in various industries and entertainment aspects like OTT and Online Gaming and gambling.
3. In 2000, Children's Online Privacy Protection Act (COPPA) took the first step at regulating personal information collected from minors.
4. California Consumer Privacy Act (CCPA) allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared.
5. According to data from the United Nations Conference on Trade and Development (UNCTAD), an estimated 137 out of 194 countries have put in place legislation to secure the protection of data and privacy, with Africa and Asia showing 61% (33 countries out of 54) and 57% adoption respectively.
6. Only 48% of Least Developed Countries (22 out of 46) have data protection and privacy laws.

II. About Drive4CyberPeace

A. **Data privacy -** #Drive4CyberPeace is an initiative that has allowed CyberPeace Foundation to gain a critical understanding of what people understand by Data privacy and protection, this has been an on-ground survey and interaction to provide a critical and holistic view of the data privacy requirements and shortcomings. The drive was aimed to create awareness around the safety & privacy of Data.

B. **Interaction -** Various Open discussions were conducted on -
   1. Confidentiality & Integrity of data.
   2. Focus on data privacy issues & rights in online domains.
   3. Drive conversations on the upcoming legislation on data protection.

C. **Route and timeline -**
   1. Phase 1
      a. The drive covered a distance of nearly 580 Km, flagging off from ISB (Indian School of Business), Hyderabad to the Indian Institute of Sciences, Bengaluru, interactions with people from different states, ages, professions, and cities were carried out in order to gain a critical understanding of what people understand by data privacy and protection. An overall on-ground interaction was done with nearly 3650 people during the course of the drive.
   2. Phase 2
      a. The campaign was taken ahead in the form of visits to various colleges and gaining inputs in different forms of engagement. The following engagements were conducted-
         (1) Veermata Jijabai Technological Institute, Mumbai - Roundtable discussions with Ph.D. scholars and senior college professors.
         (2) Shah & Anchor Kutchhi Engineering College, Mumbai - Focus group discussions and presentations with groups of college students, led by industry experts.
         (3) National Law Institute University, Bhopal - CyberPeace talks, wherein industry experts interacted with law students in an interactive panel discussion

Phase 1 Institutions

- ISB, Hyderabad
- Vardhaman College of Engineering, Hyderabad
- Ravindra College of Engineering for Women, Kurnool
- Anantha Lakshmi Institute of Technology, Ananthapur
- KSR Government Junior College, Ananthapur
- JNTU, Ananthapur
- SJCIT, Chikkaballapur
- RNS PU College, Bangalore
- Soundarya College of Engineering, Bangalore
- Ramaiah University of Applied Sciences, Bangalore
- Indian Institute of Science, Bangalore

D. Reach of the Drive -

1. Phase - 1

   Physical on-ground Interactions - 12 Colleges, 2 Villages & 1 Public Place, while interacting with nearly 3650 people.

2. Phase - 2

   a) Colleges Visited -

   (1) Veermata Jijabai Technological Institute, Mumbai
   (2) Shah & Anchor Kutchhi Engineering College, Mumbai
   (3) National Law Institute University, Bhopal

Total Tweets
5,176

Trending Duration
National (4+ hours)

Phase 1

Total Impression
3,75,25,876

Total Reach
1,85,27,076

Phase 2

Total Impression
2,78,678

Total Reach
1,37,420

III. Data Protection and Privacy in India

A. **IT Boom in India and Evolution** - India has been a country of service providers since the start of the 21st century, as the aspect of digitization was spreading out in the west, the majority of jobs were outsourced to the Asian continent and hence to India, thus allowing the Indian population to learn from the western evolution. The IT sector was booming because of technological Giants like Microsoft, Apple, Google, etc. The IT sector in India was born in the 1970s, but liberalisation provided it with the much-needed thrust, leading Indian companies like TCS opened the doors to innovation and new tools and software thus allowing the Indian consumer to get first-hand experience of the IT services.

B. **Internet Users in India** - There is no doubt that the use of technology has been accelerated due to the Covid-19 pandemic and as of today India has nearly 700 million Internet users. About 351 million of India's 692 million active internet users are in rural parts of the country, where internet penetration stands at 37%.[2]

C. **Data Usage and Consumption** - This digital age is fueled by Data, which runs the services of the IT sector. Data consumption and sharing form the basis of cyberspace. Data usage in India has risen at a CAGR (Compounded Annual Growth Rate) of 53 percent over the period between 2017 to 2021, according to a report released by Nokia.[3]

D. **Shreya Singhal vs Union of India** - The 2015 landmark judgement of Shreya Singhal vs Union of India the Hon'ble Court struck down section 66A of the Information technology Act, 2000 on account of being unconstitutional and being ultra vires to privacy. [4]

E. **Jus. K.S Puttaswamy vs Union of India** - 2018 landmark judgement of Justice K.S. Puttaswamy vs Union of India, the learned Supreme court held that Digital Privacy is an integral part of the Right to personal life and liberty and hence the same is secured and guaranteed as a fundamental right under article 21 guaranteed by Part III of The Constitution of India. [5]

F. **Governments Proactive Stances in the Cyberspace** - In recent times the Govt released a Data Protection Bill, 2021, the bill's main tenets include- Individual consent, data breach notification, transparency, purpose-based processing, technical security, and rights of individuals who part away with personal data such as name and email ID, or sensitive personal data such as a social security number. However, the same was withdrawn by the Govt in order to make the bill more coherent and congruent to the current times and technology [6]. There is no denying that with the advent of Web 3.0 various new technologies are going to come our way and hence Indian needs to secure the legal ambit in order to better protect Indian Cyberspace and in turn be a leading example for the world in terms of cyber security.

G. **Digital Personal Data Protection Bill, 2022**- The Ministry of Electronics and Information technology released the Digital Personal Protection Bill, 2022 on 18 November 2022. The bill seems to be a revamp of the older version. A data protection board will be set up for grievance redressal mechanisms and for imposing fines and penalties on data fiduciaries. The bill seems to be generic in nature as the keen ingredients like data localisation, cross-border data flow, free flow of data and right to be forgotten are not mentioned in their complete sense, thus creating a grey area for the execution of the said bill. The bill also imposes heavy penalties on data fiduciaries for non-compliance, however, the same seems harsh for start-ups and small business owners [7].

IV. On ground inputs

During the course of the drive the team interacted with various people from different and diverse backgrounds and professions. The main understanding of data privacy is based on how the individual uses the internet. As per the on-ground interaction, the following opinions were gathered from the people -

A. Majority of the people agreed to the fact that they were not really aware of the various permissions required for apps and websites to function and provide the services and thus allowing the device to grant access permissions just so that they can do the task over the app or website.
B. The platforms seek various access permissions like - Camera, location, Bluetooth, and tracking, nearly 75% of people do not completely understand how data is tracked when apps are not in use and how dangerous the third party and the apk apps can be.
C. It was seen that the majority of the college students agreed to the fact that they were aware of threats like data breach, students use data for educational and entertainment purposes, and maintain regular cyber hygiene practices as well.
D. The people from small towns and villages use the data for entertainment only and most of the people just use it because of the ease of human efforts and access to high-speed internet services.
E. The keen understanding herein is that the older generations are less aware of the data related threats as compared to the younger generations, but the younger generation though understands technology, lacks experience and hence are also victims of data related threats.
F. Majority of the people were unaware of the fact that Digital privacy is a fundamental right.
G. People who are engaged in work like cab drivers, tea stall owners, small food chains, grocery shops, guards, motor garages, and even domestic help agreed to the fact that they are unaware of the privacy breach threats and incidents and hence they often ignore the advisory messages and notifications.

Glimpses from the #Drive4CyberPeace Campaign

V. Round Table Discussion:

As a part of the drive a round table discussion was organised led by the Indian School of Business and Cyber Peace Foundation. The aim and objective of the round table was to brainstorm on different aspects of data privacy and governance. Around 90+ participants participated in the discussion led and moderated by ISB Faculties and Esteemed panellists. The different areas discussed during the discussion and its outcome helped formulate the recommendations to the policymakers.

1. Global Data Privacy scenarios with regard to potential similarities in the Indian Context

The need for Global Data Privacy has increased as the cloud perspective has increased, especially, because of the involvement of foreign industry heads and companies. As creation of data centres in India is in progress with a state-level distribution, data localization is a booming issue now as different states can have different political agendas. To counter this, a centralised system can be applied with a singular HR agenda or corporate policies centralised.

These agendas or centralised government mandates can be based on the rules that are present in USA or Europe such as GDPR. The best practices in these nations can be emulated in our country but we need to analyse our own cultures and subcultures and localise these practices. But to counter this, MNCs can arrange virtual desktops being set up to prevent data centres in India. Only deterrent to the virtual setup is the fact that it is expensive.

Indian data is extremely valuable due to the diverse and large consumer and the private sector cannot afford to ignore the Indian market due to the growing economy. This aspect is a huge asset as well as a liability, as this can cause huge privacy issues for the citizens. In order to avoid this exploitation, the government should set up laws that an industry or company not take more than the required information. Fintech Apps already go through SEBI approvals where it prevents extracting excessive information from its users.

The nations should agree on regulations for responsible online behaviour, esp., when it can result in death or major loss. The regulations should be bite-sized initially as this can leave space for adding new regulations as time passes. The governments should probably install a pre-existing software to prevent cyber-attacks such as phishing, but this can result in mass surveillance by the governments which can attack the citizens' basic right to privacy.

Governments need to focus on already established infrastructure where we can deliver information about cyber security or how to maintain data hygiene, for e.g., TV Infomercials.

2. Organisations data and data organisations-the relationships between the two

Data Organization and data privacy are impacting the individual and the group of people on really basic if there is no data privacy the all the bank related, or personal related data of an individual are not safe and foolhardy people can collude against that unique or individual and make and harmful act which we can easily prevent from making a good data protected platforms. From the individual perspective, data privacy starts with your mobile itself. When you permit an application to access all your information from your message or your contact list, you are giving the information to the application to collect data from your mobile; the individual, violating their privacy issues, is providing the data to a 3rd party. They are sometimes using is against you for a business organisation they should offer excellent good 3rd party cloud data management company & contract where they should explicitly mention that if there is going to happen any data leakage, then they are the only one who is responsible for all the losses which the company is getting because of their fault.

3. Data Use and Interpretation for different industries and how are they interdependent?

Data Interpretation helps review the data using various analytical methods to arrive at significant conclusions. The data interpretation allows researchers to classify, manipulate, and check the information. Data will likely come from multiple sources and tends to enter the analysis process with chaotic ordering. In the Banking sector, manufacturing sector etc data is used to analyse customer behaviour, likes, and dislikes; based on that, they recommend their products, the decision on customer segments, product innovation, etc.; Thus, it's very important to have regulations on exchange of data between different organisations.

4. Major tech giants drive innovation but often fail compliance, how can compliance be strengthened in the future.

Firms especially in the edtech space need to follow compliance standards such as COPPA. This is occurring due to the lack of awareness and lack of education towards the privacy standards that need to be met. During data migration tasks with respect to sensitive information such as human resource and personal details, MNC tries to wrestle with the regional laws of the country, for the data has restrictions to move into another region. GDPR and Russian databases are typical examples as per the compliance norms that the data needs to be stored within the respective geographical region. Questionnaire and Quiz are a few ways to stay abreast with the compliance standards within the organisation.

VI. Recommendations for the Indian Data Privacy and Protection regulations and policies

Cyber Peace Foundation under the capacity of a cyber laws and policy think tank proposes the recommendations for data privacy in the Indian spectrum under the following threefold aspects -

A. **Recommendations for the Government and Policy Makers** - The Govt plays a very vital and primary role in securing the data of the citizens. The Govt understands the responsibility it holds and needs to deliver and has been constantly working towards attracting new technologies to India to ensure skill development and also pushing the aspect of entrepreneurs to strengthen the aspect of self-reliance in terms of cyberspace innovations. The govt has released bills and cyber security policies which have targeted the data protection of the citizens and the govt itself. These policies have laid down SoPs, protocols, advisories, and notifications to the citizens, corporate houses, govt institutions, and organisations in order to protect the wholesome Indian Data. As per the survey and the on-ground interaction, the following are the recommended proposals to improve cyberspace.

1. **No Transactions on Public WIFI** - The govt should declare a mandate that financial transactions should not be conducted over public wi-fi's. These networks are open-ended and are more vulnerable to financial fraud, thus it is recommended to ban all transactions over open public WIFI networks or to put a cap limit on the monetary value of the transaction. Furthermore, banks should be equipped with secure WIFI for the customers to use, thus protecting the financial data by and large.

2. **Remove Auto-Detection of Credit Cards** - The govt should add a provision banning or restricting all platforms to not to store the banking details of the customer or add guidelines for a regular updating of banking details in order to prevent any third party to store or leak any banking credentials.

3. **Data Localization** - The aspects of data localization need a brief response from the govt, to ensure compliance with law of the land by the companies based abroad. Data localization will also help in strengthening the self-reliance aspect as the same will give opportunities to Indian startups and companies to create jobs in the sector of data management and protection. As data localisation increases, so will the accountability and employment opportunities.
   a. RBI Guidelines 2019 0n data localisation clearly signifies the aspect of data localisation.

4. **Compensation for data breach victims** - The victims of data breach or cybercrimes which are facilitated by data breach should be provided with compensation with respect to the volume and sensitivity of the data breached. A provision for the same can be added to the existing act and a separate schedule providing the intensity of the punishment in terms of data volume, intensity, and reoccurrence of the breach should be laid down to penalise the accused and pay compensation for his/her acts.
   a. Customer Compensation Policy- The awareness and compliance for the same needs to be increased and hence SoPs and awareness campaigns are essential.

5. **Standardisation of app parameters** - The Govt should establish concrete parameters to verify the authenticity of websites and applications. A regulatory authority should be set up which keeps a check on the privacy policies, data usage, data sharing, and originators of applications on the various platforms to ensure clean app downloading platforms. The same will also be substantially helpful in ensuring compliance by the platforms and corporate houses.

6. **Educating People on Data Privacy and Governance**- Governments need to focus on already established infrastructure where we can deliver information about cyber security or how to maintain data hygiene, for e.g., TV Infomercials.

7. **Statutory Right or Fundamental Right** - The government along with the judiciary's consent needs to lay down whether the Right to Digital Privacy is a statutory right or a fundamental right.

8. **Procedure for Insolvency** - The policymakers need to create provisions either in the existing Insolvency and Bankruptcy Act or the IT Act to address the issue of insolvency in case of data fiduciaries and the conditions/parameters to declare data as an asset.

9. **Right to Erasure** - The consumer should be given the opportunity to erase his/her data after the purpose of the processing of data is fulfilled. This will result in increased user accountability and a reduction in data breach incidents.

10. **Data Classification** - The general data should be classified in terms of criticality, vulnerabilities and usage in order to increase accountability and awareness among users and platforms.

11. **Fin-tech Data** - More diligence and strictness be followed for the management of fin-tech data

B. **Recommendations for the Corporations** - The corporate houses/platforms share an equal responsibility towards safe data management, and privacy as does a government. The platforms are the one that releases an app or website for public use and also issues the policies and the licensing agreement for the same, however, it has been found that various malicious apps make their way which in turn cause data breaches and further facilitate cyber-crimes. The corporate houses /platforms are the service providers and hence it is their moral and professional responsibility to make sure any product which comes over on their platforms should be safe for public use. These organisations provide various employment and innovation-based opportunities to the citizens but at the same time they fail or refrain from complying to the law of the land, thus keeping the aspect of data management and privacy ambiguous and in a grey area. The various technological giant corporate houses and platforms have proposed the following recommendations in order to make sure they are partners in securing and improving Indian cyberspace.

   1. **Stringent Check on Apps** - Various apps make their way on play store and app stores of different operating systems like IOS & Android. These platforms own the responsibility to verify and check apps before public release. The platforms are suggested to set up an inspection team which will be responsible for inspecting any and all apps before they are made available for public use. The same team will be also responsible to make sure the app is not violative of any indigenous policy or law. The qualifications for such inspection team members should be provided in a public notification to maintain transparency.

2. **Public Opinion Polls on the Banishment of Apps** - The platforms should conduct public polls after the launch or releasing of any app over the platform itself. This poll should reflect the users interest and opinion towards the data usage, management, tracking and privacy over the application. The poll results should be taken into consideration for removing or reintroducing any application over the platforms.

3. **Cookies Should be Rectified** - The cookies over any website or search engines should be rectified and verified to be safe for public use. The same can be done by the inspection team in order to maintain accountability and transparency of the website's activities and data utilisation.

4. **Reduction in Length of Terms and Conditions** - The terms and conditions of any website or application should be broken down into a simpler language to make sure the common public can understand it and hence the simplified terms and conditions should be made available in regional languages as well. The platforms are suggested to create a policy mandate under which they direct the app developers to create a short interactive video which highlights the various permissions and data-related terms and conditions showcasing data utilisation thus allowing better and more efficient dissemination of the privacy policies, thus easing the interpretation of the same by the citizens at large.

5. **AI to Identify Malafide and Fake Content** - The corporate houses should create a mandate of innovation in terms of Artificial Intelligence (AI) tools and software which will be better and faster in assessing and taking down malafide and fake content. This should be mentioned with respect to a time frame, defaulting to which will result in monetary fines. Technological corporate houses lead the world in terms of innovation and hence innovation for protective measures is their paramount professional responsibility.

6. **Virtual Desktops** - As creation of data centres in India is in progress with a state-level distribution, data localization is a booming issue now as different states can have different political agendas. MNCs can arrange virtual desktops being set up to prevent data centres in India. Only deterrent to the virtual setup is the fact that it is expensive.

7. **Automated Data Management** - Automated data management avoids tedious manual work and data privacy issues. However, setting up an effective and adequate data processing automation system requires deep reflection and a global strategy. However, this time invested will be recovered mainly once the system is in place. Automation can remove much human power and keep it more private and protected. In the automation system, we don't need to check the log or what is happening in the background as it is the preassigned instruction that which method is following, so there are fewer chances of data leakage. Automating data processing saves costs both directly and indirectly. First, you reduce the overall salary costs since part of the tasks are carried out automatically. Then, your employees gain in productivity. And the company is getting more data privacy. With better tools, you get better results.

8. **Mandated Parental Control Mode** - All platforms and application developers should create a parental control mode that allows the parents or guardians to monitor the child's online safety and activities.

9. **Social Media Safety** -

    a. **Child Safety-** The usage of social media by young children cannot be ignored and hence the platforms can create separate portals for children which is regulated by a more strict and stringent check on the content & community guidelines. (Blanket of restriction)

    b. **Women's Safety-** The aspect of women's safety needs to be taken into account by creating an option for women users to reduce interactions with strangers, thus creating an option for online safety.

10. **Tech Control Policy** - The corporate houses are recommended to regularly update their respective Tech Control Policy in order to maintain strict cyber security.

C. **Recommendations for the Users/Netizens** - The netizens are by and large the users of cyberspace, the user is the prime contributor towards data consumption. The user is the end consumer of all the data over applications and websites, in which they consume some and contribute some. The contributed data is primarily used for data tracking and utilisation the same can be in two forms - Entertainment, Professional & Personal. The user is the one who suffers due to any irregularity in the data sharing and tracking policies and patterns. Data breach targets individuals and organisations which are in turn working towards creating and perfecting the services for the user, hence any breach directly or indirectly affects the user in terms of cybercrimes. The user plays the main role whether in the case of any app or website launched by the platforms or in the case of any new law and policy by the government, hence netizen participation is of paramount importance to create a safe and secure cyberspace that protects the user's data effectively and efficiently. The following recommendations are proposed for the user, these can be undertaken by NGOs & Civil society organisations, and stakeholders, which will result in wholesome civic involvement and improvement of cyberspace.

1. **Greater Vigilance** - The public should be trained to be more vigilant about sharing personal pictures, videos and banking credentials, etc. The public must abide by the golden rule of not trusting anyone online and should not click on unknown and suspicious links. Better awareness and information regarding the security blockchain payment system and end-to-end encryption is the need of the hour.

2. **Opening Avenues** - More avenues need to be explored and generated to tap into the talent looking to make a career in the cybersecurity domain which will in turn increase civic participation and furthermore strengthen the aspects of entrepreneurship and innovation among the netizens.

3. **Active Reporting Duty** - The netizens own a vital responsibility towards reporting the illicit content and actors over the platforms more actively. The right to privacy is guaranteed by fulfilling active cyber safety duties, thus reporting over platforms is a civic duty for all netizens which secures their right to privacy.

4. **Conditions Over Convenience** - The users need to be vigilant in their online activities and hence should practise reviewing conditions over convenience, this means that the netizens should not blindly grant various apps and websites access permissions without reviewing the terms and conditions of the same. Users often blindly agree to terms and conditions in order to just simply use the app or website without realising the serious implications this can cause, hence it should be taken up as a cyber safety protocol and practice.

5. **Strong Password Practices** - The public must be educated to master the art of password creation, the password should be unique with different letters and numbers. Passwords can be changed at regular intervals and the use of biometric features for the protection of devices.
6. **Literature Acknowledgement** - The practice of reading the privacy terms and conditions needs to be incorporated as part of cyber hygiene. The user reads all terms and conditions in case of a physical contract or agreement, hence the same should be encouraged in terms of apps and content downloads.
7. **Investing in Start-ups** - The boom of cyberspace is yet to be witnessed by the Indian Consumer and creating incentives and campaigns to encourage netizens to invest in Indian tech-based start-ups will result in a wholesome self-sufficient and reliant Indian cyberspace.
8. **Speak Reality, Not Hearsay** - The users should be encouraged to discuss any instance of cybercrime in order to increase mass awareness and busting of various myths and misconceptions.
9. **Digital Footprint Retracing** - Netizens should be encouraged to track their digital footprints in order to be aware of their activities and any instances of data breach or cybercrime.
10. **Sustainable Cyber Development** - The netizens should be critical in understanding the needs of the next generation hence the tech or policy developed in today's time should not be a threat to future generations.

VII. Conclusion

The future holds a lot of new and emerging technologies like blockchain and metaverse, these will further take data consumption and utilisation to a new level and scope, hence it is critical for the nation to come up with effective Data privacy and management policies, laws and strategies with an outlook far into the future. The Government, Corporate houses, and the users are equal recipients of contributing towards data privacy and protection, all these actors share and own respective and different responsibilities, each of them being of critical importance towards securing Indian Cyberspace. The government being the torchbearers of laws and policy needs to incorporate the necessities and requirements of the citizens and further provide parameters for operations for corporate houses and platforms, in this regard the active and efficient actions by the Government have been seen lately in form of the new Information Technology Rules, 2021, Intermediary Rules, 2022 and the latest Indian Telecommunication Bill, 2022 which shows the government's proactive vision for the wholesome development and protection of the cyberspace. The platforms being the service providers have the onus of maintaining a clean and safe platform, although the primary role of a corporate house is profit-oriented, they cannot neglect the aspect of protection of their users and hence each corporate house and platform lie in the middle of the regulations & laws laid by the government and the data consumer, i.e., the end user. Corporate houses and platforms need to improve their compliance and platform safety to be in congruence with the data privacy and protection needs of netizens. The end user being the netizen, contributes towards data and is also the victim in case of any irregularity or breach by the corporate houses or the Government, hence netizen's participation plays a vital role in safeguarding cyberspace, hence it of paramount importance that the netizens exercise their digital rights while simultaneously fulfilling their digital civic duties, which will result in transparency and easier comprehension of laws, policies and new technologies.

India as of now stands at a critical juncture in regard to laws and policies for data privacy, protection, and management, with major technological advancements heading our way it is vital that the nation lays down elaborative policies with an eye over the future in order to create a self-sufficient and reliant Indian cyberspace, thus governing the actions of the corporate houses, platforms and the end user while simultaneously providing for grievance and redressal mechanisms under the Judicial system to maintain a separation of power in the democratic spirit.

VIII. References and Links

1. Global Penetration Index -
https://www.internetworldstats.com/stats.htm

2. Internet users in India Global Penetration Index -
https://www.internetworldstats.com/stats.htm

3. Data Consumption in India -
https://www.indiatimes.com/technology/news/average-mobile-data-consumption-india-564559.html#:~:text=Highlights.per%20user%20in%20the%20year.

4. Shreya Singhal vs Union of India -
https://indiankanoon.org/doc/110813550/

5. Justice K.S Puttaswamy vs Union of India -
https://indiankanoon.org/doc/127517806/

6. Withdrawing Personal Data Protection Bill, 2019 -
https://www.nytimes.com/2022/08/04/business/india-data-privacy.html

7. Digital Personal Data Protection Bill, 2022 -
https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

Disclaimer

Contributors of the Project

Honourable Mentions

Mr. Vajapeyajula Srinivas
AVP, Chase Bank

KSR Government Junior College, Ananthapur

Bukkarayasamudram Village, Ananthapur

Uparpalli Village, Ananthapur

SRTC Bus Stand, Ananthapur

CyberPeace | Foundation

CyberPeace Foundation (CPF) is a global civil society organization, think tank of cybersecurity and policy experts with the vision of pioneering CyberPeace Initiatives to build collective resiliency against cybercrimes and global threats of cyber warfare. CPF is involved in Policy Advocacy, Research and Training related to all aspects of CyberPeace and Cyber Security. Key areas of CyberPeace Foundation's work are in Technology Governance, Policy Review and Advocacy, Capacity and Capability creation and building through partnerships with various government organizations, academic institutions and civil society entities.

MISSION

To work with netizens, national and international institutions to facilitate inclusion, security, stability and trust

VISION

Peaceful, Responsible and Inclusive Cyber Space

MEMBER OF

नीति आयोग

Global Compact Network India

ICANN AT-LARGE

RANSOMWARE TASK FORCE

COALITION AGAINST STALKERWARE

End Violence Against Children THE GLOBAL PARTNERSHIP

CyberPeace
Foundation

www.cyberpeace.org | secretariat@cyberpeace.net | +91 953 445 6565

FOLLOW US FOR MORE

/CyberPeace Foundation /cyberpeacengo /CyberPeace TV