PEGASUS SPYWARE: A VIOLATION OF RIGHT TO PRIVACY AND A THREAT TO SURVEILLANCE LAWS IN INDIA

Written by ***Jonus D'Souza***

5th Year B.A LL.B Student, V.M. Salgaocar College of Law Miramar Panaji, Goa, India

ABSTRACT

Technology has progressed at such an advanced stage which makes it possible for anyone to spy into our private lives. The concept of Pegasus Spyware and its ill effects has gained significance in today's time. Pegasus is a sophisticated spyware tool that has been widely used to target individuals around the world which forms a major concern by infringing and compromising an individual's privacy and security. The Spyware is designed to infect, monitor and gather data of mobile devices by exploiting software vulnerabilities and using advance techniques to avoid detection. The Pegasus spyware outrage gives an account of the various issues pertaining to the infringement of the fundamental right to privacy guaranteed under the Indian Constitution and throws light upon the inadequacies in the surveillance laws which deal with such circumstances. In the year 2021 there were allegations and speculations with regards to use of Pegasus spyware to gather and monitor crucial information of various individuals holding different positions in the country. Such Spyware not only raises concerns about privacy but also about violation of human rights and freedom of expression. It is very crucial that rightful and appropriate steps are taken to protect the privacy and security of individuals in a country by implementing strong data protection laws and regulations and ensuring that surveillance tools are in accordance with the law and with appropriate oversight and accountability mechanisms. There arises a need for an express legislation which will govern data protection and a surveillance mechanism which will preserve the rights of a citizen and hold the wrongdoer accountable for such breach. The Current study focuses and explores the capabilities and impact of the Pegasus spyware and highlights and analyses the various issues and laws dealing with surveillance in India.

Keywords: Pegasus Spyware, Right to Privacy, Breach of Privacy, Surveillance Laws.

"Privacy is an inherent human right and a requirement for maintaining the human condition with dignity and respect."

-Bruce Schneier

INTRODUCTION

The concept of privacy is of old origin and has evolved over time. Privacy means the freedom from interference or intrusion or it can be said the state of being free from unwanted intrusion. Advancement in technology has made it easy to easily spy into one's life i.e., to access one's personal data without consent, data gathered is misused at a great extent. Privacy has been recognized internationally as Human Rights under "Article 12 of UDHR". Today the world has been increasingly interconnected and it becomes important to explore the right to privacy concept and know what are the various challenges faced in this digital age. This concept has evolved over time at a great extent from common law principles to modern constitutional protection.

The misuse of Pegasus spyware by various governments has raised many concerns. The use of this spyware has led to allegations of Violation of privacy and human rights. Due to unprecedented dependency on the internet and our devices for work related or financial and personal needs our information in the online database is at stake. We never know when our personal data will go into the hands of professional hackers. The use of this spyware also sparked a global debate about the ethics of surveillance of government on individuals.

OBJECTIVES

1) To Outline the various problems and impacts of Pegasus spyware on the right to privacy.
2) To study and analyse Constitutional provision of right to privacy and various laws dealing with Surveillance.

RESEARCH METHODOLOGY

The Research Methodology adopted for this research paper is Doctrinal research. The Researcher has collected secondary data from different Articles, Books Journals, Case studies etc. and the same has been analysed.

MEANING OF RIGHT TO PRIVACY

According to Black's Law Dictionary**, "*Right to Privacy means the Right to be let alone or the right of a person to be free from any unwarranted interference*"**. "The right to privacy is a basic right that grants individuals the autonomy to keep communications, personal information, personal life free from undue interference and it also protects freedom of speech and expression and personal dignity".

IMPORATANCE OF DATA PROTECTION

The primary goal of data protection regulations is to guarantee that data is not stored without authorization and that it is not disclosed or used by unauthorised persons. Technology is advancing at such a tremendous pace, and we are adapting to the changing needs. With the introduction of Artificial Intelligence (AI) and now being widely used by individuals and companies there arises a possibility of data breach and there can also be inferences of sensitive information of individuals. Data protection will ensure to protect individuals' privacy by controlling the acquisition and processing of data of users. Data protection ensures security of sensitive information from unauthorized and unlawful access, breaches and cyber-attacks. Data protection laws ensures that the governments and organizations fulfil their obligations with privacy and data security of personal information. Concrete privacy laws will foster the confidence and trust of individuals thereby adequately protecting one's personal data. Data Protection also gives protection to Cross border Transfers i.e., when data is transferred to countries with different legal frameworks it will ensure that personal data is protected. Lastly, as it is said data is the new oil, it is crucial that for maintaining privacy, ensuring security,

building trust, promoting compliance, and addressing various privacy issues which is a need of this hour in this data driven world.

INTERNATIONAL POSITION

Right to privacy has also been internationally recognised, it makes it way in many international laws and conventions. Article 12 of the UDHR 1948 states, "*that a person shall not be subjugated to arbitrary interference with his privacy*"[i]. Article 17 of the ICCPR 1966, mentions that "*a person's privacy should not be subjected to arbitrary intrusion*"[ii]. Similarly, the ECHR[iii] mentions that, "*every person has a right to protect his private family life and correspondence*". In the year 2018 to regulate and consolidate data protection with EU, the European Union enacted GDPR[iv], this regulation is said to be one of the concrete privacy laws in the world. It focuses on how individuals' personal data in the EU may be processed and transferred.

INDIAN LEGAL FRAMEWORK

In India, the Right to Privacy appeared a little later than it was in other nations. Over the last 60 years of development, the idea of the right to privacy has changed, and the court has played a significant role in interpreting it. In India the Constitution and statues give protection to Right to privacy of individuals as well as personal data. The right to privacy is not specifically stated in the Indian constitution, but it has been incorporated into Article 21 through judicial interpretation. In the case of ***R. Rajagopal Vs. Union of India[v],*** "*the Supreme court recognized the right to privacy, and stated that it is a right to be let alone guaranteed to the citizens of this country under Article 21 of the Indian Constitution*". In the case of ***"People for Civil Liberties Vs. Union of India"[vi],*** "*the validity of section 5(2) of the Indian Telegraph Act 1885 was challenged. The Apex Court held that tapping of Telephonic conservation that is private in nature amounts to violation of right to privacy*". *The Apex court also in this case framed rules with regards to interception of data*. Also, In the case of ***Govind Vs. M.P[vii],***"*the right to privacy was recognized as a fundamental right by the Supreme Court".*

In the case of **"*MP Sharma Vs. Satish Chandra*"[viii],** "the court reasoned that the Right to Privacy was not a fundamental Right protected by the Indian constitution". In the case of *"**Kharak Singh Vs. State of UP**"[ix],* "the Court also stated that the Indian Constitution does not guarantee the right to privacy and hence Privacy is not a Fundamental Right".

Justice Puttaswamy Vs. Union of India[x]

The Honourable Supreme Court overruled the above two judgements. The 9 Judge Bench on 24th August 2017 held that, "the right to privacy is an integral and intrinsic part of the right to life under Article 21 of the Constitution". In this case retired Justice Puttaswamy filed a case in the Supreme court Questioning Aadhaar's legitimacy as its use violated or infringed the right to privacy. The key issue in this case was whether the right to privacy is a fundamental part of the right to life and personal liberty given under Article 21 of the Indian Constitution, as well as the freedoms guaranteed by part III of the Indian Constitution. According to the Supreme Court, "the right to privacy is not absolute right and is subject to reasonable restrictions". The Court also stated that "there must be a balance between individual interest and legitimate state interest". The Apex court laid down "*a triple test which needed to be satisfied for judging the permissible limits for invasion of privacy which included the test of Legality, Necessity and Proportionality"*. It was also mentioned that "The Right to Privacy imposes on the state a duty to protect the privacy of an individual"[xi].

If the above triple test is applied in the present scenario the essentials are not fulfilled. It defies the first essential of legality as it not an existing or binding law. Second, it also defies the essential of Necessity as its aim is certainly not for a legitimate use or purpose. Third, the essential of proportionality is also defied as there is no rational connection between the aim and means to achieve it. Thus, it can be concluded that the Spyware is a direct violation of our right to privacy as it has failed to meet the three-fold test laid down by the Supreme Court[xii].

SURVEILLANCE LAWS IN INDIA

The primary goal or the main aim of surveillance laws is to curb unlawful and unauthorised surveillance. The two salient laws dealing with Surveillance in India are as follows:

1) Telegraph Act[xiii]

The Act mentions the government's authority to take over licenced telegraphs. It also states when it can allow interception. It states the various circumstances when the government can intercept calls. It includes "the security of the state, the interests of India's sovereignty and integrity, friendly relations with foreign states, or public order, and preventing incitement to commit an offence, which can only be done in the event of a public emergency or in the interest of public safety"[xiv]. Rule 419A was introduced to the Indian Telegraphs Rules, 1951 granted under the Indian Telegraph Act 1885 in the year 2007, which said that orders for communication interception should only be issued on the orders of the Secretary in the Ministry of Home Affairs[xv].

2) IT[xvi] Act 2000

The IT Act is an important Act dealing with Indian Cyber laws. The primary object of the Act is to carry lawful, trustworthy and genuine digital and online transactions, it is a legislation dealing with data protection. The Act has undergone several amendments. This Act contains 13 chapters and 90 sections. Few provisions deal with individuals privacy and are not exhaustive in nature. Following are some of the important provisions: Section 43 of the Act talks about that if a corporate body who is handling, dealing or possessing any personal data is negligent in maintaining security practices will be held liable to pay compensation to the affected person. Section 69 of the Act gives the power to the competent authority for monitoring, decryption or intercepting of any information in the interest, sovereignty or integrity of India or be it the security of state or be it any friendly relations with foreign states or public order or be it the purpose to prevent to incitement to commission o or investigation of an offence which is cognizable. Section 72 of the Act mentions, “the Penalty for disclosure of information without consent and breach of privacy”. Section 43A of Act states “that a corporate body will be liable to pay compensation if it fails to protect data”. Section 72A of the Act mentions “the Punishment for disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of a lawful contract”. Sections 43A and 72A are punitive in nature. The above 2 provisions were added by the IT (Amendment) Act, 2008. The protection of "Sensitive personal data or information of a person" is mentioned in Rule 3 of the **IT Rules**[xvii], some of which includes protecting login credentials, biometric

information, details of financial information, medical records, or any other sensitive personal data[xviii].

REPORT OF THE GROUP OF EXPERTS ON PRIVACY

Under the chairmanship of Justice AP Shah, the former Chief justice of Delhi High Court a report was prepared by experts highlighting the key privacy issues in the year 2011. The report contained recommendations on national privacy principles which should be taken into consideration when creating a privacy law. The report gives nine important principles necessary to be considered while formulating the proposed framework for a privacy Act. First, the principle of Notice mentions that it is the duty of the data collector to give notice or notify individuals before collecting any personal information. The second principle is the principle of choice and consent, which asserts that when it comes to the supply of personal data, individuals must be given the option to opt in or opt out. Without the individual's consent, no data should be collected or processed. Third, the collection limitation principle stipulates that only for an indicated purpose the data controller shall collect information. Fourth, it states that when the data collector gathers and analyses data, it should ensure that it is adequate and relevant to the objectives for which it is gathered. Fifth, the principle of access and correction stipulates an individuals right to view their personal information kept by the data controller also allowing to make corrections or erase the information. Sixth, the information disclosure principle emphasises the data controller's ban on exposing personal data to other parties. The seventh security principle states that while personal data is in the possession of the data controller, responsibility for ensuring the security of all personal data acquired should be taken into consideration. The eighth principle of openness, states that a data controller is required to provide as much information as feasible about the practises, processes, policies, and systems that it deploys to comply with the National Privacy Principles. Ninth, principle of accountability, which holds the data controller accountable for carrying out actions that comply with the previous eight principles. Such recommendations must include procedures for implementing privacy regulations, according to the law[xix].

OVERVIEW OF THE PEGASUS SPYWARE – IS IT ETHICALLY CONCERNING?

It is said that Pegasus Spyware has analysed over thousands of mobile devices worldwide. Pegasus is a member of the malware family known as spyware, which was created by the cyber security company NSO group., an Israeli technology firm stands for N- Niv Carmi, S- Shalev Hulio, O- Omri Lavie who are the three founders of the company. The spyware is made to hack into cell phones in order to get personal information without the user's knowledge. The Spyware works in 3 modes that is it first targets a digital device next step it infects the device by capturing data and last it tracks by reporting the information collected from the users device. The spyware infects both operating systems i.e., Android and IOS. The spyware has the ability to gain access to contact lists, files stored in device, messages, photos, videos it also has the ability to record audio, video and also can track the location of the user without its consent. The spyware uses zero click attack technology by which it gains control over a device without human interaction. The spyware was sold to many governments across the globe for the purposes of protecting national security and preventing terrorism. Unfortunately, this spyware is used for wrongful surveillance means thereby violation our right to privacy. Once a device is infected with this spyware it becomes extremely difficult to detect and remove the same, this is the reason why it is said to be a highly sophisticated type of spyware.

PEGASUS ISSUE IN INDIA

In July 2021 there were speculations of an issue which was brough to light regarding the use of Pegasus Spyware designed by Israeli Cybersecurity company NSO Group which was suspected to be used by the Indian Government to Track and target digital devices of the Ministers, Activists, opposition leaders and journalists. According to NYT Report it is said that "India purchased the Pegasus spyware in the year 2017 as part of a larger arms deal with Israel".[xx]. Amid these speculations the central government denied all allegations made by global media investigation agencies with regards to the use of Pegasus spyware. Multiple writ petitions were filed before the Supreme Court alleging the unauthorised and unlawful surveillance of personal information of digital devices by the government violated the

Fundamental Rights of Citizens. The matter was taken up in the case of, "***Manohar Lal Sharma Vs. Union of India and Ors."***[xxi] The petitioners in this case requested for a judicial probe to look into if the government used the spyware on its citizens. It was also submitted that the spyware "curtailed the freedom of speech and expression and violated the right to privacy of citizens". The respondent i.e., the Union of India was asked to respond to the allegations made. A limited affidavit was submitted which completely denied all allegations made against the Union. It as stated by the court that limited affidavit was insufficient. The respondent further stated that detailed reasons cannot be put forth as it would be a threat to the National security and Defence of the Nation. The court was not satisfied by the reply and it appointed a Technical Committee which had the role to investigate the truth and falsity of the allegations made by the petitioners. After being given an extension, the committee ultimately presented its report. The report stated that out of the 29 phones which were examined, malware was found only in five of them, but there was no definite proof that it was exclusively Pegasus spyware. Further it stated that the Government did not co-operate with the technical committee in the scrutiny of the digital devices to detect the Pegasus spyware. The Supreme court in this case also gave few recommendations for strengthening cyber security. It included creation of an exclusive primary agency to probe threats and issues to cyber security, also it was recommended that laws should be amended to protect citizens against illegal surveillance. Also, it was stated that no private party will be permitted to carry out snooping[xxii].

KEY ISSUES CONCERNING THE PEGASUS SPYWARE / IMPACT OF PEGASUS SPYWARE

1) Violates Right to Privacy

Pegasus Spyware can infiltrate data on one's devices without the consent of the user. Collecting, processing, monitoring and gathering images, audio, documents, location without the knowledge of the user is said to violate the right to privacy.

2) Lack of Accountability and Monitoring

Pegasus spyware is raising doubts about the regulation of surveillance technology. There are worries that governments and agencies may be using spyware without the required legal

authorisation which in turns leads to abuse of power and violation of our human rights. Hence there is lack of transparency and accountability in the system.

3) Difficulty in Detection and Removal

Once a user's phone gets infected with this spyware it is becomes very difficult to detect and remove the same, that is why it is said to be a highly sophisticated spyware. That's how the spyware uses zero click technology to capture personal data without human intervention.

4) Legal and Ethical Concerns

The deployment of Pegasus has sparked discussions about the ethics and legality of monitoring methods. Concerns have been raised about the need for clear regulations governing creation, sale, and use of surveillance technologies as well as the need to strike a balance between individual privacy rights and national security.

5) Curtails freedom of press

Pegasus also has major impact on journalism. Pegasus is used to target journalists which usually undermines or supresses the freedom of press.

6) Loopholes in Legislations

Weak laws and legislations affect our right to privacy and thereby allows easy surveillance. Types of interception, the level of detail of the information that can be intercepted, and the level of cooperation from service providers makes it easier to break the law and support government monitoring.

PDPB[xxiii] Bill 2019- ANALYSIS

The "Minister of Electronics and Information Technology" tabled the "Personal Data Protection Bill 2019" in the Lok Sabha on December 11th, 2019. The Bill has previously undergone amendments. The Bill was withdrawn reason being that new legislation on data protection will be presented. Following were some of the important features of the Bill: It aims to describe the flow and use of personal data, as well as to establish a trusting connection between the individuals and organisations that handle the data. It seeks to safeguard the rights

of persons whose personal information is being processed. It aims to provide a framework for technological and organisational measures in data processing, as well as rules for the affiliation of social media intermediaries, cross-border transfers, and the liability of businesses processing personal data.

Some of the features of the bill are, it states, "that no personal data should be handled by any individual unless for a specified, explicit, and legitimate reason, thus prohibiting the processing of personal data. Furthermore, it states that, "collecting of personal information should be limited to that which is essential for the processing of such information, resulting in a limitation on personal data collection and when personal data is being collected, serving of notice is mandatory". When it comes to the quality of personal data processed, the data fiduciary is obligated to take the necessary care to guarantee that it is correct, up-to-date, comprehensive, and does not contain any misleading information. Personal data should not be kept for longer than necessary and should be erased at the end of processing. It states that consent is required for the processing of personal data. The Bill specifies numerous reasons for processing personal data without consent. Personal data is categorized as sensitive personal data in the draft, It stipulates the processing of children's personal data and sensitive personal data, and every data fiduciary is obligated to treat children's personal information in a way that preserves their rights and serves their best interests. It proposes the requirement for every data fiduciary to have a privacy by design policy. The law prohibits the processing of sensitive personal data and critical personal data outside of India, as well as the circumstances for transferring sensitive personal data and important personal data outside of India. It states that, "any government agency under the control of the central government may be exempt from the Act's applicability in the interest of India's sovereignty and integrity, the security of the State, friendly relations with other countries, and public order; or for preventing incitement to the commission of any offence punishable by law"[xxiv]. The Bill proposes the formation of a Data Protection Authority of India, which will be a legal entity comprised of a chairperson and no more than six full-time members. The bill specifies the authority's powers and functions. The authority may take discretionary action against data collectors or processors. It states that in the event of a violation of privacy, a complaint can be brought against a private organisation as well as the government. It also states the consequences for violating the terms of this Act. The Bill seeks to establish a

Data Protection Authority Fund to cover the authority's expenditures and to carry out its tasks"[xxv].

DPDP BILL 2022…. A WAY FORWARD? -ANALYSIS

After the PDPB Bill 2019 was withdrawn in the year 2022, a new bill was presented "**DPDP Bill 2022**[xxvi]". The main objective of the bill is to protect the privacy of persons or users concerning their personal data. Unauthorized use of personal data can cause grave harm to individuals and companies hence protection of personal data is in need of the hour. Some of the salient features of the bill are as follows:

The Bill defines key terms such as Data Fiduciary, Data Principal, and Personal Data. The Bill applies when personal data is gathered online from data principles and when digitized personal data is obtained offline. The Bill discusses the various functions of data fiduciaries, including the need that personal data be processed only with consent or deemed consent. It requires the data fiduciary to notify the data principle when personal data will be acquired. It states that the consent granted by users can be revoked at any moment, just as it was given. It states that no conditional services can be provided in exchange for the processing of any personal data, and that a data fiduciary must refrain from holding personal data. Data fiduciaries should have an acceptable grievance redressal procedure in place to address the issues of data principals. It also states that data fiduciaries must get verified parental consent before processing any personal data of a child. The Bill discusses the various rights and responsibilities of data principals. These rights include the right to personal data information, the right to rectification and deletion of personal data, the right to nominate, and the right to grievance redressal. The Bill states that personal data can be transmitted outside of India only with the consent of the central government and according to the terms and conditions. The bill proposes the formation of the DPBI[xxvii], which will be responsible for determining failure to comply with the provisions of this Act and can impose appropriate fines in the event of non-compliance. Penalties of up to Rs. 250 crores are included in the Bill[xxviii].

NEED TO PROTECT OUR PRIVACY IN TODAYS DIGITAL AGE – SUGGESTIONS

Protecting our Right to Privacy in today's digital era is of paramount importance as technology continues to advance. Following are some of the suggestions to Protect our right to privacy:

1) **Strong Data Protection Laws:** Enacting robust data protection laws is necessary which clearly highlights the rights, responsibilities of users relating to storage, collection, and usage of personal data. These las should be fully dedicated to protect the privacy of individuals. Also, these laws should be applicable to Governments and private entities.
2) **Transparency and User Consent:** Clear and Informed consent must be obtained from individuals before collecting one's data. Users ought to be fully-informed about the purposes for which the data will be used, as well as with whom and how it will be shared. There should be clear transparency in the collection, usage and storage of data collected.
3) **Robust Encryption System:** Encryption protects users' privacy by concealing users personal data. This will ensure data confidentiality along with proper authentication and will ensure integrity. Implementing robust encryption for data will help to prevent data breach and unauthorized access.
4) **Creating Awareness about Privacy Risks:** Proactive steps can be taken to create awareness about privacy and implications associated with it. This will help the users to understand and educate themselves about the potential risks and will help to take active measures to protect their privacy.
5) **Regular Review and update of Laws:** There should be regular review and update of privacy laws with the pace of evolving technology and changing privacy concerns.

CONCLUSION

It is said that the freedom that its citizens hold forms an important feature of a democratic Nation. In conclusion, to evolve the jurisprudence of Right to Privacy in the Constitution of India it took almost a span of 60 years. the spyware effectively and definitely compromises the privacy and security of individuals which has brought to light the significant implications. The Pegasus is such a sophisticated spyware which makes detection almost impossible. The recent

spyware outbreak has created a panic situation and it makes us vigilant about the need for a proper legal framework to deal with the advancement of surveillance measures across the globe. Though the IT Act 2000 and its rules contains provisions for data protection it appears to be inadequate. Every country should have dedicated cyber security laws. We never know that the future wars will not be physical wars but will surely be cyber wars. And the Pegasus is an eye opener for us which makes it mandatory for the need of a legal framework to prevent cyber warfare situations in the coming future.

As stated by the Apex court in the Pegasus case that getting immunity from judicial review by citing the reason of national security concern doesn't mean that the government will get blanket immunity If the government or private entity uses such technologies for unlawful surveillance purposes, violating the rights of a person, they should be held accountable for the same. Information collected by surveillance should be used for reasonable purpose. There also arises a need that individuals must be vigilant about such potential spyware attacks and take just and proactive measures to secure its digital devices from unlawful surveillances.

REFERENCES

[i] Universal Declaration of Human Rights 1948.

[ii] International Covenant on Civil and Political Rights 1966.

[iii] Article 8 of The European Convention on Human Rights 1950.

[iv] General Data Protection Regulation.

[v] AIR 1995 SC 264, (1994) 6 SCC 632.

[vi] AIR 1997 SC 568, (1997) 1 SCC 301.

[vii] AIR 1975 SC 1378, (1975) 2 SCC 148.

[viii] (1954) 1 SCR 1077.

[ix] 1964 SCR (1) 332.

[x] Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC.

[xi] Ibid

[xii] Bhasin, Rehan. Pegasus: "An infringement of right to privacy" burnishedlawjournal 2 no. 3 (2021): 721

https://burnishedlawjournal.in/wp-content/uploads/2021/08/Pegasus-An-infringement-of-right-to-privacy-by-Rehan-Bhasin.pdf

[xiii] Indian Telegraph Act 1885

[xiv] Section 5(2) of The Indian Telegraph Act 1885

[xv] Indian Telegraph Act 1885.

[xvi] Information Technology Act 2000

[xvii] Information Technology Rules 2011

[xviii] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[xix] Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, "Report of the Group of Experts on Privacy", Planning Commission (CIT&I Division), Government of India, 16 October 2012.

[xx] India Bought Pegasus as Part of Larger $2 Billion Deal with Israel in 2017, Claims "NYT" Report. (n.d.-b). The Wire. https://thewire.in/tech/india-bought-pegasus-israel-nyt-report

[xxi] WP (Crl) 314/2021.

[xxii] Ibid

[xxiii] The Personal Data Protection Bill 2019 (Bill No. 373 of 2019)

[xxiv] Ibid

[xxv] Bill No. 373 of 2019.

[xxvi] The Digital Personal Data Protection Bill 2022

[xxvii] Data Protection Board of India

[xxviii] The Digital Personal Data Protection Bill, 2022.