IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA PRIVACY AND ITS NATIONAL AND INTERNATIONAL PERSPECTIVES- A FOCUS ON INTERNATIONAL TRADE AND THE INTERNET OF HEALTH THINGS.

Bhawna Tyagi, Dr. Akbar Khan,

Research Scholar, Associate Professor,
Law Department,
ICFAI Law School IFHE (Deemed to be University under section 3 of the UGC Act, 1956), Hyderabad, India

Abstract: **The authors of this paper have made an effort to discuss both nationally and internationally historical perspectives while addressing the difficulties that every country faces. California Consumer Privacy Act of 2018 and Federal Trade Commission were also brought up by American authors while addressing the General Data Protection Regulation 2018 of the European Union (FTC). Authors began with the MP Chandra v. Satish Chandra case while discussing the national viewpoint before eventually arriving to the PDPB (Personal Data Privacy Bill 2019) later in the 2021 Data Privacy Bill (DPB).**

Index Terms - Data Privacy, Internet of Health Things (IOHT), International Trade, GDPR, Schrems I, Schrems II, CCPA, Data Privacy Bill 2021

Introduction

I. International Perspective-

The right to privacy is established by international law and is now widely regarded as one of the fundamental rights to which every human being should be entitled. Through Article 12[1] of Universal Declaration of Human Rights (UDHR) in year 1948 for the first-time privacy was recognised globally. International Covenant on Civil and Political Rights in year 1966 highlighted the concept of privacy through Article 17 guaranteed individuals' protection of their personal sphere as broadly conceived.[2] Everyone has the right to the protection of the law against such interference or attacks". Despite that this provision is lacking of binding power, it is acknowledged as a general principle under international law and have been incorporated in international treaties, human right instruments, and national constitutions.[3] This rule, however, has a broad scope and is insufficient to address data protection in the digital age. While there is no obvious distinction between the definitions of privacy and data protection, it could be said that privacy is a broader concept than data protection. As a result, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 is introduced as a more explicit instrument that specifically governs personal data. It comes out to be the first legally obligatory document on data protection.

The 1980 OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data ("OECD Guidelines")[4]. The OECD Guidelines endorse eight principles, applicable in both the public and the private sector, and also encourage countries to

[1] Universal Declaration of Human Rights, Article 12 (Dec. 10, 1948) (No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks)

[2] International Covenant on Civil and Political Rights, Article 17,(Dec. 16, 1966) (No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation)

[3] International & Foreign Legal Research Department, *International and Foreign Cyberspace Law Research Guide*, Georgetown Law Library: 2019, P. 7.

[4] Guidelines for the Protection of Personal Information and Transborder Data Flows of Personal Data ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT [OECD] (Sept. 23, 1980)

develop their own privacy protection frameworks along them. These eight principles are: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards principle; (6) openness; (7) individual participation; and (8) accountability.[5] The 2005 APEC Privacy Framework ("Privacy Framework")[6] is in many ways similar to the OECD Privacy Guidelines[7].

In this regard, the author would like to point out that European countries have the most comprehensive data protection strategy. The establishment of the European General Data Protection Regulation (GDPR), a regional regulatory treaty that comes into place in May 2018, confirms this.[8] In 2018 GDPR, the EU's new data protection legislation, has the same aim as the 1995 Data Protection Directive: to standardize the protection of individuals' basic rights and freedoms in processing activities and to ensure the free movement of personal data between EU Member States. In Article 5[9] of the regulation, it enshrines seven key criteria for the lawful handling of personal data, namely: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality (security); accountability. Compliance with the spirit of these principles becomes the main fundamental building block for the practice of a good data protection.[10] In 2018, Europe's GDPR brought in new regulations on an individual's right to his personal data, raising digital privacy expectations to new heights. GDPR aims to provide customers more control over the acquisition and use of their personal data. In the event of a violation, fines may be imposed. Organizations that violate GDPR must face a fine[11] of more than EU 20 million or 4% of their yearly global turnover. As a result, the EU's new privacy regulations are being taken seriously. GDPR's main goal is to ensure that business' actions and policies comply with privacy regulations. In the EU, a company that uses its customers' personal data to provide services, sell products, or keep track of them is known as a data processor. With the implementation of GDPR, people now have rights to access the information that businesses hold about them, as well as new requirements for corporations to properly handle their data and a new system of fines.

In the context of the extraterritorial application of the GDPR and what has been particularly controversial, as exemplified by Schrems I and more recently in 2020 by Schrems II, is the possibility of the European Commission to find that a third country offers "an adequate level of data protection." With this, the EU reviews the partner country's protection standards unilaterally. This would mean that personal data could flow freely from the EU (and, as members of the European Economic Area, Norway, Liechtenstein, and Iceland) to a third country without the need for additional safeguards,[12] or, in other words, transfers to the third country would be assimilated to intra-EU data transmissions. So far, the European Commission has recognised Andorra, Argentina, Canada (commercial entities), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and the United Kingdom of Great Britain and Northern Ireland and Uruguay as having appropriate data privacy standards, and has negotiations with South Korea are still ongoing[13].

---

[5] Guidelines for the Protection of Personal Information and Transborder Data Flows of Personal Data Organization for Economic Cooperation and Development [OECD] (Sept. 23, 1980)

[6] Asia-Pacific Economic Cooperation, APEC Privacy Framework (2005)

[7] The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?, 71 PRIV. L. & BUS. (2004).

[8] European Union, General Data Protection Regulation, https://gdpr-info.eu

[9] European Union, General Data Protection Regulation, Article 5 (2018) [Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').]

[10] ibid

[11] European Union, General Data Protection Regulation, Article 83 (2018)

[12] European Union, General Data Protection Regulation, Article 45(1) (2018) (A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation)

[13] . Adequacy Decisions, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_e

Privacy and data protection have not been a negotiation topic during the Uruguay round; the WTO law has not, as of the date of this writing, undergone any changes that reflect their growing importance or digital transformation in general.[14] Despite this, and although WTO law represents a "hard" form of international law, it does include certain mechanisms meant to reconcile economic and non-economic interests, international commitments, and domestic values and sensitivities.[15] Overarching market access and national treatment commitments is GATS Article XIV, which provides a list of general exceptions to a Member's GATS commitments.[16]

Key amongst these mechanisms are the "general exceptions" formulated under Article XX of the General Agreement on Tariffs and Trade of 1994 ("GATT")[17] and Article XIV of the General Agreement on Trade in Services ("GATS").[18] These Articles allow WTO Members to take actions that would otherwise be against their responsibilities, provided that those actions are not veiled trade restrictions. The potential that Article XIV of the GATS may permit both the retention of current data limits and the implementation of new data restrictions based on grounds of privacy protection is particularly intriguing for the debate in this Article. The flexibility provided by the GATS, which enables WTO Members to customise their obligations in the various service sectors, keep a significant amount of policy latitude, and maintain and introduce some restrictive measures, is not covered in this Article.[19]

The scholarly discussion over whether Article XIV of the GATS applies to privacy protection issues will undoubtedly continue as long as there is no relevant case law and as the topic's significance grows. For the time being, it is crucial to emphasise that the general exception clause found in Article XIV of the GATS is a good illustration of both the flexibility of WTO law and its potential to intervene in domestic affairs to penalise WTO Members and draw a distinction between legitimate protection and illegal protectionism. The interpretation of Articles XX of the GATT and XIV of the GATS remains crucial despite the impasse at the WTO and the crisis in its dispute resolution system.

II. National Perspective

Human society has always assumed that the demand for secrecy, privacy, and personal space has a basic origin. Over time, many sectoral laws and regulations have also included appropriate defences and safeguards for data privacy. Human society has always assumed that the demand for secrecy, privacy, and personal space has a basic origin. The concept of privacy backed its origin from the time of pre-Independence. In 1948 at time of pre- Independence the Constituent Assembly's initial attempt to safeguard an individual's right to privacy against undue governmental intrusion came from Mr. Kazi Syed Karimuddin, who proposed an amendment to do so in line with the American and Irish Constitutions. 8 judges' bench in *MP Sharma v Satish Chandra* case in year 1954 held that "In every system of law, the state has the absolute right to search and seize property in order to ensure social security, and this right must be subject to legal restrictions. There is no justification for importing a completely different fundamental right into the Constitution through some strained construction process when the Constitution's framers thought it appropriate to not subject such regulation to constitutional limitations by recognising the fundamental right to privacy, analogous to the American Fourth Amendment".[20] 6 Judges bench in *Kharak Singh vs The State of U P & Others* case in year 1962 held that held that "the right of privacy is not a guaranteed right under our Constitution, and therefore the attempt to ascertain the movements of an individual is merely a manner in which privacy is invaded and is not an infringement of a fundamental right guaranteed in Part III (fundamental rights)".[21]

The renowned Supreme Court decision in K.S. Puttuswamy v. Union of India, known as the "Puttaswamy Judgement," "identified 'privacy' as integral to the right to life and liberty, provided by Article 21 of the Constitution of India, thereby creating 'right to privacy' a fundamental right, and established the groundwork for a single statutory law for the protection of data in India. The Puttaswamy Judgment touches on safeguards for people in the private realm while primarily addressing the range of rights of a citizen as opposed the State. The Supreme Court cited well-established precedent to declare that the State had a positive responsibility of upholding and safeguarding this dignity and connected the value of privacy to the value of person dignity."[22] As a result, the Puttaswamy Judgment serves as the foundation for both the ban of privacy-violating State action and the State's obligation to regulate private contracts and private data exchange, both of which are necessary to protect individual privacy.

As a result, the Sri Krishna Committee was established and the Draft Personal Data Protection Bill was released in 2018. The Personal Data Protection Bill 2019 ("PDPB") was introduced in the Rajya Sabha by the Ministry of Electronics and Information Technology in December 2019 after being amended in response to input from stakeholders and industry.

This iteration of the PDPB suggested changing India's legal system to control data sharing in commercial agreements. It established strict compliance requirements for all types of personal data, expanded the range of individual rights, established a central data

[14] World Trade Report 2018: The Future of World Trade: How Digital Technologies are Transforming Global Commerce, WORLD TRADE ORG. (2018)

[15] Mira Burri, The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation, 51 U.C. DAVIS L. REV. 65, 87–88 (2017).

[16] GATS , Article XIV

[17] General Agreement on Tariffs and Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A.

[18] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B.

[19] Pierre Sauve & Anirudh Shingal, Reflections on the Nature of Preferences in Services, 45 J. WORLD TRADE 953 (2011)

[20] MP Sharma v Satish Chandra 1954 AIR 300, 1954 SCR 1077

[21] Kharak Singh vs The State of U P & Others 1963 AIR 1295, 1964 SCR (1) 332

[22] K.S. Puttuswamy v. Union of India (2017) 10 SCC 1

protection regulator, established data localization requirements for specific types of sensitive data, and imposed significant financial penalties for noncompliance, among other things.

The PDPB was, however, brought to the Joint Committee of the Parliament ("JPC") for review in 2019 due to a number of implementation-related issues. The JPC then took almost 2 years, when the world was experiencing a pandemic, to review and discuss the subtleties of the PDPB.

In July 2020, a committee of experts assembled by MEITY released a study on the framework for the governance of non-personal data ("NPD Report"). The goal of the NPD Report was to develop a framework for businesses, startups, and the government to access the economic, social, and commercial worth of non-personal data. The committee received approximately 1,500 answers to the NPD Report from diverse stakeholders, and revisions were made as a result of the input. The same committee issued a revised NPD Report in January 2021 that clarified how the PDPB and the Non-Personal Data Governance Framework would work together as well as limiting the scope and purpose of exchanging non-personal data.

The JPC subsequently filed its updated report and draught of the bill in November 2021. The Data Protection Bill 2021 ("DPB"), the PDPB's new name, included a number of major amendments. The law's extension to include non-personal data as well as personal data was a significant move. In order to mitigate data breaches, the DPB also established strict reporting requirements for data breaches, regulations of hardware manufacturers, a mechanism for certification for all digital and IOT devices, and an additional compliance measure requiring consultation with the Central Government for cross-border transfers of sensitive personal data. The DPB also provided for a staggered implementation wherein the Central Government may designate various dates for passage of different provisions.

It was anticipated that the DPB would be presented to Parliament during the budget session held in February 2022, but the new version of the legislation received harsh criticism and pushback from a number of stakeholders, including members of the JPC and domestic and international business houses, for, among other things, being more concerned with safeguarding state interests than it was with safeguarding individual data and privacy.

As a result, the future of the DPB is now uncertain. According to numerous media news sources, the Indian Government is likely to abolish the DPB in favour of brand-new data protection laws. According to media sources, the IT Act may also undergo revisions to meet the demands of the nation's shifting technology environment.

In an effort to capitalise on the commercial potential of public sector data in the context of the uncertainties surrounding India's data security policy, MEITY produced a draught India Data Accessibility and Usage Policy ("Data Usage Policy") in February 2022. The main goal of the Data Usage Policy is to recognise open data as a valuable public resource and address existing data accessibility issues. Open data is any dataset that is freely available for anybody to use, reuse, and redistribute. All data and information produced, gathered, generated, or preserved by the Indian Government, whether directly or through authorised agencies by various ministries, departments, organisations, agencies, and autonomous bodies, is subject to the Data Usage Policy.

The Data Usage Policy is a commendable first step in revealing the economic worth of public sector data, and it has the potential to allow the business ecosystem to significantly benefit from the planned data sharing. However, the lack of a thorough privacy and data protection law in India as well as a lack of infrastructure support would make it impossible to assign responsibility and offer remedy for privacy violations or data breaches from a practical standpoint.

It seems that India's five-year effort to establish a strong rule for privacy and data protection has temporarily slowed down. However, according to the measures put out by the Indian government on the revision of the IT Act and the framework for exchanging data in the public sector, significant progress will be made in creating an all-encompassing data governance framework for India in the coming months. Additionally, it would be fascinating to observe the redesign of the data protection system, which will be a challenging challenge and need prompt engagement from business parties.

Given that India is one of the world's major data marketplaces, a thorough data protection and governance policy would undoubtedly have an impact on and make a significant contribution to the development of the global data governance environment.

III. Legal Framework

1. International Trade and Privacy Law

1.1 European Union- General Data Protection Regulation (GDPR)

On May 25, 2018, the General Data Protection Regulation (GDPR) of the EU became effective. While maintaining the general regulatory approach of its predecessor, it replaces the prior legal framework for the EU that goes back to 1995. The GDPR also adds a number of additional compliance duties, including harsher penalties than those permitted under the earlier framework from 1995. The EU data protection law has a dual purpose: on the one hand, it aims to facilitate the free flow of personal data, but on the other hand, it subjects that flow to compliance with legal requirements derived from the fundamental rights character of the right to privacy and the right to protect individuals' personal data.[23] The European Union's (EU's) Charter of Fundamental Rights (the Charter), which

[23] Lynskey O. The foundations of EU data protection law. Oxford, 2015

guarantees the right to privacy (Article 7 of the Charter)[24] and the right to the protection of personal data (Article 8 of the Charter), serves as the foundation for the fundamental rights nature of EU data protection law (Article 8 of the Charter)[25].'

The GDPR adopts an "omnibus" approach[26], which refers to its application as a general legislation covering a broad range of processing activities and actors (including public agencies and commercial organisations), as well as an expansive definition of what comprises the processing of personal data. Contrast this with the US legal system, which has a sectoral approach and does not have a comprehensive (federal) data protection legislation, such as by individually regulating children's privacy or insurance and health privacy.[27]

Scope of GDPR-- The GDPR is applicable to both commercial and public enterprises. In contrast, specific regulations exist for EU institutions, organisations, and agencies (Article 2(3) GDPR)[28]. Personal data processing is covered under the GDPR (Article 2 GDPR)[29].

Here, it's important to take into account the concepts of personal data and processing. In order to clarify the concept of personal data and outline the legal requirements for its processing, the GDPR makes use of four different categories:

1. Personal data

2. Special categories if personal data

3. Pseudonymous data

4. Anonymous data

Special categories of personal data, also known as "sensitive personal data," as defined by Article 9[30] GDPR, include: (i) racial or ethnic origin; (ii) political opinions; (iii) religious or philosophical beliefs; (iv) membership in a trade union; (v) genetic data; (vi) biometric data; (vii) data pertaining to health; and (viii) sex life or sexual orientation. These data come with a greater level of risk for the data subject, thus any organisation processing them needs to take additional compliance measures. The notion of special categories of personal data includes data elements that can serve as substitutes for certain traits. For instance, some dietary needs in passenger name records were designated sensitive data because they would reveal information about the religious views of the data subjects. 14 Article 9(1)(j[31]) GDPR provides derogations that may be adopted by virtue of EU or Member State national law in the context of research. According to Article 9(4)[32] of the GDPR, Member States may also keep or enact certain restrictions on the processing of genetic, biometric, or health data. Therefore, under the GDPR, Member States have the discretion to permit or prohibit the processing of certain kinds of data, which might have a significant influence on how research is carried out.

Principles Relating to Lawful Processing- The standards allowed for the authorised processing of personal data are outlined in Article 5[33] of the GDPR.[34] Which Includes-

1. Lawfulness, fairness and transparency: When one of the six legal bases stated in Article 6 GDPR is used, processing of personal data is justified.[35] Fairness and openness requirements state that data subjects must get a thorough explanation of the nature and extent of the processing, as outlined in Articles 12 to 14 of the GDPR.[36]

2. Purpose limitation: Data can only be processed for a particular purpose, which must be disclosed to the data subject, in accordance with the transparency principle. If the conditions outlined in that article are met, some derogation is allowed under Article 89 GDPR[37] in the context of research, allowing for further processing.

3. Data minimisation: According to this idea, controllers must keep their data collection and storage to a minimum.

4. Accuracy: The correctness of the data must be guaranteed by the controller.

[24]European Convention on Human Rights, Article 7 (1950)
[25]European Convention on Human Rights, Article 8 (1950)
[26] Supra 23
[27] European Union, General Data Protection Regulation, Article 1(2) and (3)
[28] European Union, General Data Protection Regulation, Article 2(3) (2018)
[29] ibid
[30] European Union, General Data Protection Regulation, Article 9 (2018)
[31] ibid
[32] Supra30
[33] European Union, General Data Protection Regulation, Article 5 (2018)
[34] European Union, General Data Protection Regulation, Article 5 (2018)
[35] European Union, General Data Protection Regulation, Article 6 (2018)
[36] European Union, General Data Protection Regulation, Article 12 and 14 (2018)
[37] European Union, General Data Protection Regulation, Article 89 (2018)

5. Storage limitation: According to this concept, controllers must designate the period of time after which data is removed. If the conditions outlined in Article 89 GDPR are met, certain derogations are allowed in the context of research.[38]

6. Integrity and confidentiality: The integrity and confidentiality of personal data must be guaranteed in order to comply with this principle. It relates to the responsibilities for data security, putting in place suitable technological and organisational safeguards, and the need to notify the supervisory authority and/or data subjects of data breaches in specific situations as outlined in Articles 33 and 34 of the GDPR[39].

1.2 USA- California Consumer Privacy Act of 2018 (CCPA)

The California Customer Privacy Act, which went into effect on January 1st, significantly advanced efforts to safeguard consumer data (CCPA). As one of the biggest economies in the world, California is the first state to enact comprehensive legislation pertaining to the protection of consumer data privacy. The CCPA comes after Europe's well-known General Data Protection Regulation (GDPR), although no other governments have passed laws resembling it as of yet.

While the CCPA may be an outlier in the United States for the time being, it and other legislation of a similar nature are expected to lead to even more regionalized consumer data protection laws. Consumers are asking for more transparency about who has access to and uses their personal data. It's wise to think about what this implies for your business as organisations start to feel the effects of the penalties and fines associated with GDPR non-compliance — and as you ponder what laws may be on the horizon.

By ensuring that all data initiatives are centred on security, organisations may assist in reducing the difficulties posed by upcoming regulations. Organizations should think about privacy and data governance in every part of their companies and make important choices with data protection in mind rather than responding to each new piece of law as it is passed.

Federal Trade Commission (FTC) - Federal Trade Commission Rules (FTC Rules) prohibits unfair and deceptive practices on the market, including cases when companies fail to keep their promises listed in privacy policies.

The diffusion of free data flow commitments in free trade and investments agreements can have hazardous consequences for the regulatory consistency of a third country's data protection framework. If a third country commits to free cross-border data flows in a free trade agreement with yet other countries, it is risking its strategic ability to obtain a finding of adequacy by the Commission in order to freely receive personal data from the EU or risk losing the earlier afforded adequacy status. Pursuant to Article 45(2) (a) of the GDPR, the Commission would assess the rules for onward transfer of personal data to another third country. For example, the Commission's finding that Japan ensures an adequate level of protection does not extend to onward transfers of personal data pursuant to the APEC Cross Border Privacy Rules. Through the backdoor, the strategy to liberalize free data flows is starting to upset approaches based on mutual recognition of data privacy laws, as practised in the EU and many other countries.[40]

In the interest of EU law consistency, the Commission's position on personal data protection in its external trade policy and the preference given to the regulatory mechanisms of the GDPR must be welcomed. This starkly contrasts with the perceived 'gold standard' for digital trade as championed by the USA and other developed countries prioritizing trade liberalization and the removal of 'unnecessary' restrictions of cross-border data flows. What is certain is that the confrontation between cross-border flows of personal data in a connected world and the fundamental rights to the protection of personal data and privacy in the EU will not subside anytime soon. Future directions in international trade diplomacy should aim to establish realistic coordinates for digital trust in cross-border trade in services, which cannot realistically be parted from individuals' positions of rights as guaranteed in their countries

1.3 India:

Personal Data Protection Bill- Draft Personal Data Protection Bill, 2019 places limitations on transfer of personal data. It brings in concepts like data localisation and data mirroring to this effect. Local data storage requirement for digital payments has been mandated by RBI directive on payment data storage. Draft e-commerce policy[41] explicitly mentions certain categories of data on which cross-border flow restrictions shall apply. It suggests creation of a legal and technological framework which can provide the basis for imposing restrictions on cross-border data flow from certain sources. A panel headed by Kris Gopalakrishnan is working on the Indian government's cloud computing policy. The policy will be the latest in a series of proposals that seek to spur data localisation in India.

[38] ibid

[39] [39] European Union, General Data Protection Regulation, Article 33 and 34 (2018)

[40] Svetlana Yakovleva* and Kristina Irion, Pitching trade against privacy: reconciling EU governance of personal data flows with external trade, International Data Privacy Law, 2020, Vol. 10, No. 3

[41] //dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

The Department for Promotion of Industry and Internal Trade (DPIIT) released a draft e-commerce policy, which addresses 5 other issues besides 'Data'. It attempts to address regulatory gaps from the PDPB, as well as ensure harmony amongst different policies in this regard.[42]

Consumer Unity and Trust Society (CUTS) - Consumer Unity and Trust Society (CUTS) is a global independent non-profit policy research and advocacy organization since 1983.[43] It is registered under the 'Rajasthan Societies Registration Act, 1958 (Rajasthan Act No.28, 1953), Foreign Contribution (Regulation) Act, 1976, and comes within the ambit of section 80-G, Sub (5) of the Income Tax Act.[44]

They prepared a memorandum for the Standing Committee on Information Technology (2017-18) on Citizens' Data Security and Privacy, highlighting consumer perspective.[45] CUTS recommended the Committee to adopt and institutionalise undertaking Regulatory Impact Assessments (RIA) and Competition Impact Assessments (CIA), while framing/providing any suggestions on the policy, regulatory and/or legislative framework regarding 'Citizen Data Security and Privacy'.[46] In 2018, we undertook a consumer perception survey (in line with our recommendations mentioned above) in India to better understand users' perspective, experience and expectation of privacy and data protection and accordingly provide policy and practice suggestions to improve privacy and data protection in the country.[47] The survey reported that although 90% users are aware of their right to privacy, they don't take measures to protect it- do not read privacy policies or use data protection tools. This is despite users perceiving unauthorized data collection as the highest risk. The suggestions include improving transparency and user capacity on privacy and capacity building issues.[48]

Foreign Trade Policy (FTP) - The fundamental foundation of policy and strategy for encouraging exports and trade is provided by India's Foreign Trade Policy (FTP). It is revised on a regular basis to adjust to the shifting domestic and global environment.

The current Foreign Trade Policy (2015–20) places a strong emphasis on increasing India's market share in current markets and goods while also examining potential new markets and products. The Foreign Trade Policy of India also includes assisting exporters make the most of GST benefits, closely monitoring export results, enhancing cross-border trade convenience, raising revenue from India's agricultural exports, and promoting exports from MSMEs and labor-intensive industries. Additionally, the DOC has worked to engage states as active export partners. State governments are consequently actively creating export plans based on the advantages of their particular sectors.

A plan to treble India's exports by 2025 was envisioned by Shri Suresh Prabhu, then minister of commerce and industry, in 2018. For important industries such gems and jewellery, leather, textiles and clothing, engineering, electronics, chemicals and petrochemicals, pharmaceuticals, agricultural and related goods, and marine products, the plan includes developing a commodity-specific strategy. The North American Free Trade Agreement (NAFTA), Europe, North East Asia, ASEAN, South Asia, Latin America, Africa and WANA, Australia, New Zealand, and CIS will all be covered by territory-specific strategies.

2. Privacy and Internet and Health Things

The Internet of Health Things promises to revolutionize healthcare in terms of improving individual health and wellness, home care, residential care, and acute care. The idea is to rely on a multiplicity of sensor-based systems to predict and prevent disease, provide personalized healthcare, offer wellness monitoring, and give support to formal and informal caregivers[49]. The IOHT has been made possible because of the concurrent development of sensor technology, data transmission, and storage technology together with new search and artificial-intelligence techniques[50]

2.1 International Perspective

HIPPA and GINA- Privacy Rights Conflict with Unwarranted Access- Genetic privacy has long been considered a healthcare problem under HIPAA, say studies by the National Academy of Sciences and the National Human Genome Research Institute (NHGRI).[51] Genetic information is protected by HIPAA safeguards if it is kept by a healthcare provider, health plan, or healthcare clearinghouse that is covered by HIPAA.[52] Healthcare provider, health plan, and healthcare clearing house are not the respective categories under which DTC firms fall.[53] The necessity of privacy in the genetic field is also mandated by the Genetic Information Non-discrimination Act (GINA), a federal law that forbids employers, employment agencies, labour unions, and joint labour-

[42] //dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf
[43] www.cuts-international.org
[44] ibid
[45] Memorandum for The Standing Committee on Information Technology (2017-18) on Citizens' Data Security and Privacy.
[46] ibid
[47] Supra 45
[48] CUTS' Networking Profile 2017
[49] Ahmad Akl, Autonomous Unobtrusive Detection of Mild Cognitive Impairment in Older Adults, 62 IEEE Transactions On Biomedical Engineering 1383 (2015)
[50] Cathal Gurrin Et Al., Digital Enlightenment Yearbook: Social Networks And Social Machines, Surveillance And Empowerment 49–73.
[51] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-19, 110
[52] HIPAA Privacy Rule 2 (2003)

management committees from releasing genetic information. Laws governing genetic privacy, however, have mostly followed health information rather than genetic information used for identification.

The NHGRI claims that a few court decisions have influenced and moulded the genetic privacy regulations governing the use of genetic information as personally identifiable information in the United States[54].

The three most important laws are generally regarded as ECPA, HIPAA, and GINA. While the ECPA addresses law enforcement access to information, it does so to a considerably lower extent than the GINA or HIPAA with regard to genetic privacy.[55] A DOJ official must approve the application for the court order permitting the interception of wire or oral communications in order to get an ECPA interception legal order.[56] The method is only applicable where there is a reasonable suspicion that electronic or wiretapping eavesdropping would result in the discovery of evidence of a federal crime.[57]

2.2 National Perspective

Personal Data Privacy Bill - A "Personal Data Privacy Bill" and the ITA 2000 revisions were created in 2006 and even presented to the Parliament. The ITA revisions later became law in 2008, but the Privacy Bill expired. Since then, further privacy bill draughts have been presented to Parliament, but none of them have been able to get support since they directly conflicted with the national security concerns raised by "interception of communication" and the installation of Aadhaar

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011- Any business organisation or body interacting with a person's SPDI is subject to these regulations. In order to develop data management, privacy, and security policies, guidelines, and patient health records in compliance with legislative provisions, the government established the National Electronic Health Authority of India in 2015.

Digital Information in Healthcare Security Act, 2018 (DISHA)- It was proposed by the Parliament to encourage and support India's adoption of international e-health standards. In India, the new law has yet to take effect. The National Health Stack initiative, put out by NITI Ayog, aims to develop digital health records for every person by the year 2022.

Privacy Data Protection Bill 2021- The Data Protection Bill, 2021 defines "health data" as "sensitive personal data" and lists "health data" as information about the physical or mental health of the data principal, including records about their past, present, or future health, information gathered during the registration process for or delivery of health services, and information connected to the delivery of particular health services.

Except from the healthcare business itself, which would be severely impacted by the Act's implementation, it seems doubtful that the sector-specific strategy presently suggested in the HDSPA targeting just the privacy and security of health care data will face significant resistance. While the larger hospital chains are likely to put the HDPSA's provisions into practise, there will be a large number of smaller nursing homes, local doctors' offices, pharmacies, and mobile app companies that deal with health information that will be unable to do so and will continue to operate in a non-compliant manner.

The Health and Family Welfare department of the Union Government is working on the HDPSA (Health Data Privacy and Security Act), which is anticipated to take a lot of inspiration from the HIPAA (Health Insurance Portability and Accountability Act) of the USA. Around 1996 saw the creation of HIPAA, which was then updated/modified by the HITECH Act (Health Information Technology for Clinical and Economic Health Act). Some people who have been monitoring HIPAA and its implementation for more than ten years believe that India is precisely following the same development route as HIPAA.

Electronic Health Record Standards by National Health Portal (NHP India)- Security and Privacy standards- The Security Standards and the Privacy Standards are inescapably connected. Any health record system must have security measures in place to guarantee that the information is accessible when required and that it is not improperly utilized, disclosed, accessed, altered, or destroyed while being kept, retrieved, or transferred. Together with the Privacy Standards, the Security Standards establish the necessary safeguards and controls. Entities in the health sector that must adhere to the Privacy Standards must also adhere to the Security Standards.

When adopting security measures, organisations must take into account a number of aspects. It is up to each company to decide how a healthcare provider will meet the security criteria and what technologies it will employ. An organisation must take into account its size, complexity, and capabilities when choosing which security measures to implement. It must also take into account its technical infrastructure, hardware, and software security capabilities, the cost of specific security measures, and the likelihood and severity of any potential risks to the E-PHI it stores, retrieves, and transmits.

[54] Privacy in Genomics, NAT'L HUM. GENOME RSCH. INST.
[55] 18 U.S.C. § 2516
[56] ibid
[57] § 2511(2)(i)

Purpose of the Security Standards

The security standards require healthcare providers to implement reasonable and appropriate administrative, physical, and technical safeguards to:

- ensure the confidentiality, integrity, and availability of all the E-PHI they create, transmit, receive, or maintain
- protect against reasonably anticipated threats or hazards to the security or integrity of their E-PHI
- protect against uses or disclosures of the E-PHI that are not required or permitted under the Privacy Standards
- ensure their workforce will comply with their security policies and procedures

IV. Suggestions and Recommendations

Some ideas can help to improve this system after a detailed review of data privacy and protection rules and compliance challenges for IOHT-based systems. These suggestions aid in overcoming healthcare data security challenges brought on by problems with legal framework compliance.

- **Fines and Penalties-** IOT devices collect a lot of data, and the use and access of that data come with a number of privacy hazards. Particularly, identification of specific individuals and behavior monitoring are significant issues. A significant quantity of personal data is collected and stored as IoT device adoption grows in the healthcare industry. There is a requirement for new privacy protections. With remote monitoring, the health data gathered from gadgets like Fitbit and Jawbone may be utilized to identify illness correlations and novel treatment alternatives.

- **Data Anonymization-** The majority of the data collected from the environment by IoT devices is sent via a router or other intermediary device for processing. Since the storage capacity on the devices is constrained and cannot support large headers like those used for Internet Protocol IPv6, a variety of protocols and compression techniques are employed throughout this procedure. Since this communication reduces safety hazards, this data is cleaned as near as possible to the device that originated it.

- **Healthcare System Design-** The healthcare system should be created such that it offers the controls in an intuitive fashion. An end user must always have complete control over the obtained data, including the ability to share it with or not. The user should always have the option to know who is in possession of his data, what information has been gathered, and how it will be used to fulfil the original, lawful purpose;

- **Privacy Policy design-** Consumer hardly reads privacy policies for this reason:

- consumer friendly language is critically necessary.
- Concise privacy policies that are readily understood by the consumer.
- Blanket privacy policy is insufficient for consumer to understand the privacy rights.

- **Privacy by Design-** A crucial element incorporated into the whole IoHT core system is privacy, which is built into the architecture. The system engineering process must start with the implementation of the privacy safety architecture. User interactions or web interfaces are used to operate the medical equipment. When creating device interfaces, there are no privacy protection rules accessible. Web-based interfaces have a number of weaknesses that make them vulnerable to data leakage and information leakage attacks. Due to their tiny size interfaces, the majority of gadgets lack authentication capabilities or have default passwords that are challenging to type.

- **Communication Security-** In IOT healthcare devices, a variety of communication protocols are employed. Data privacy regulations do not offer any particular requirements for protocol security, what kind of encryption or anonymity standards should be used for IoT devices, which have limited memory and processing power. In particular for usage in hospitals, these privacy regulations should offer clear policies regarding the communication security of these devices.

- **Dispute Resolution-** There is a need to settle local and global disagreements over data protection. Healthcare data privacy rules are implemented in many forms on a national and international level. What potential legal ramifications could arise if a citizen's medical information is handled in a foreign nation or state where different data privacy rules are in effect? These conflicts ought to be settled in accordance with national healthcare regulations;

- **Awareness Programs-** Awareness programs are very significant to highlight the importance of data privacy, especially in the healthcare sector. IT staff, management staff, and other related staff of a healthcare facility should be aware and carry out the practices of secure processing of healthcare data. They must be aware of the consequences in the case of data leakage and what penalties they would be charged in the case of carelessness. Doctor and emergency response teams should be trained for the secure usage of their devices (i.e., laptops and cellphones, etc.) linked to healthcare systems, and they should share their experiences and difficulties while using these devices securely with healthcare organizations.

V. Conclusion

This paper we presented the details about International and National perspective of privacy regulation with respect to International trade and Internet of Health Thing. In concerned with International perspective we discussed about GDPR, CCPA, FTC, HIPPA and GINA. Finally while covering national perspective, we discussed about Data protection Bill 2021, Consumer Unity & Trust society, Federal Trade Policy, IT Rules 2011, DISHA 2018 and Electronic Health Record standards by NHP.

As future work, we plan to enhance the Data privacy and security in each and every sector. PDP was introduced in 2019 and further was revised based on the suggestion in year 2021 is yet to see the light of the day. They are with the parliamentary committee; various suggestions have been made are needed to be incorporated in the Bill. Its high time India comes out with the Data protection and security legislation with the stringent section with regard to Industrial, International Trade and Health sector. Even the processing Data by foreign procuring (Trans-border Data processing) in consensus with the GDPR provisions, which imposes hefty compensation and Penalties for erranding parties. Any violation of the provision of the mentioned law shall meet with the stringent action against violation, beside prescribing provision for maintain the highest standards for encryption of Data.

The digital environment in which commerce today takes place was obviously not anticipated by international trade law, which is why it needs to play catch-up. However, the query is: How? This essay makes the case that the international trading community should learn from the flops and deadlocks in earlier discussions on digital commerce. The international trading community should concentrate on establishing fundamental framework rules to make multilateral regulations more compatible with digital commerce rather than continuing to argue about conceptually difficult but practically inconsequential matters. It should also concentrate on the biggest non-tariff trade restrictions. The WTO will continue to run the danger of losing relevance in the digital era unless and until this happens.

Large prospects are presented by the healthcare industry's digital transformation, especially in light of the ageing population's potential to put even the most effective medical systems under pressure. Data-driven technologies like the IOHT have dangers, but there are solutions to reduce those risks. More than ever, governments must create regulatory frameworks that encourage data-driven innovation while boosting public confidence in technology. The false dichotomy between privacy and technology, which implies that people must forgo their privacy in order to profit from technology, has to be disproved in this case.

VI. Limitation of Study-

In this context, a doctrinal technique that relies on secondary sources has been used. Finding out the precise number of difficulties in international trade, the influence of privacy laws on each country, and the Internet of Health Things are not practicable or practical enough.

VII. Implication and Future scope of the study-

The purpose of the study is to ascertain how privacy policies have changed society and how well they safeguard the data and personal information of any individual or business. In the comparison section, the privacy laws in India, the USA, and Europe are evaluated. Additionally, every component of development must be laid down. The study helps the researchers learn more about the topic and draw logical conclusions through the evaluation in their own research effort to determine the causes of the differences in their growth through Privacy protection.