Page 1331 - 1340 **DOI:** *https://doij.org/10.10000/IJLMH.113938*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 6

2022

Privacy and Data Protection Issues in Over-The-Top (OTT) Platforms: An Analysis

PRIYESH PATHAK[1]

ABSTRACT

In this paper analysis is done of the Privacy And Data Protection Issues in OTT Platforms. The meaning of Privacy And Data Protection and OTT is covered here. The paper is also discussing the concerns regarding the Privacy and Data Protection in OTT and the methods to mitigate it is also being discussed. Then the present regulatory framework with respect to India is being dealt with here. It also gives an explanation of relevant laws and court rulings. Protecting people's "data" is the goal of "data protection." This "right to privacy" has been declared to be a "fundamental right in India " as a consequence of court rulings. Over the top (OTT) content providers are streaming media services that are provided to consumers directly over the Net. It sidesteps cable, telecast, and satellite tv. Some of the most significant security issues affecting the OTT are being covered. Then the present regulatory framework are being discussed and then concluded with the suggestions to overcome the threats to Privacy And Data Protection Issues in OTT.

I. INTRODUCTION

Over the top (OTT) content providers are streaming media services that are provided to consumers directly over the Net. It has also been utilized to refer to the "no carrier cell phones, where all communications are charged as data, avoiding monopolistic competition, or apps for phones that transmit data in this way, including both those that replace other call methods and those that update software." OTT sidesteps cable, telecast, and satellite tv portals, the businesses that typically behave like a console or supplier of these materials. This phrase often is frequently used to refer to "SVoD (subscription-based video on demand)" service which provide accessibility to filmmaking & tv programs.The most common ways to access OTT services include webpages access in desktops, applications on portable devices (such as cellphones and tabs), streaming devices (including apple tv , chromecast etc.), or TVs with built-in Android Tv interfaces. The "right to privacy" has come to be widely viewed as a core "human right," and under India's Constitution's "Article 21," it has additionally been acknowledged as such. Privacy rights are closely related to data protection, which has become incredibly difficult to maintain in this contemporary, globally connected world. Nowadays OTT platforms cannot avoid taking

[1] Author is a student at Hidayatullah National Law University Raipur, India.

 [ISSN 2581-5369]

data security and privacy safeguards. The corporate image as an OTT service supplier may suffer as a result of security breaches, piracy, & cybercrime. In order to secure customer information, additional content, and the network's source code, special attention must be paid to such areas. Although it has been highlighted that Today's legal system has provided the "Right to Privacy" its fullest assistance and that significant steps have been taken to prevent data theft and the misuse of "sensitive information," more progressive developments still are needed to expand the scope of data protection in the present society & protect Indian citizens' rights to privacy. These times, overall pace increased in the utilization of media on OTT is concerning. Since these services had became the person's preferred medium, addressing privacy issues like data intrusions, data piracy, & accountability are becoming crucial business drivers in businesses throughout sectors.Since major online corporations take good care to handle customer information properly, data privacy &security have become primary concern of online organisations.OTT streaming services suppliers, who are now major participants in the media & entertainment industries, emerged around the same time as legislative & ethical developments in data security. Customer information has served as the cornerstone upon which businesses & services like "Netflix, Hulu, and Amazon Prime Video have been built." They use learning algorithm to examine customer watching patterns & preference in being able to aid the supplier in making aimed choices regarding creating contents & licencing. This is critical that each of the stakeholders must comprehend the overall amount in which they could utilise customer information without infringing "personal data as even more media and entertainment businesses" are entering in "OTT" space.

(A) Objectives

The objectives of this paper is to study about the Privacy And Data Protection Issues In Over-The-Top (OTT) Platforms and to analyse the issues regarding it.

(B) Research question

What are the Privacy And Data Protection Issues In Over-The-Top (OTT) Platforms? Whether there are legislations governing the Privacy And Data Protection Issues In Over-The-Top (OTT) Platforms ?

(C) Research methodology

This study that was done is doctrinal in nature. Both descriptive and analytical approaches are used in the process. The creation of such a work was mostly aided by literature as well as other resources, notably from different websites. To comprehend the idea at its most fundamental level, information across numerous sources has indeed been collated & examined. At which

 [ISSN 2581-5369]

appropriate citations have been included, that has aided to give the research an elevated finishing.

(D) Scope of study

This study primarily focuses on the Privacy And Data Protection Issues In Over-The-Top (OTT) Platforms where the meaning and concept of privacy and data protection is being discussed with respect to OTT platforms and the legal status regarding the same is also highlighted. At last the conclusion , findings and suggestions are given.

(E) Limitation

This research is limited to books available, journals, statutes , legislations and other online sources. Wherever the statistics are mentioned that referred to the sources are cited in footnotes.

II. MEANING, CONCEPT OF PRIVACY, DATA PROTECTION & OTT

The ability of an individual or indeed a body to make information private & hidden from everyone is referred to as privacy. It is protected by Article 12 of the UDHR,[2] which states that "no one has the right to have their privacy, communication, or family interfered with, nor is anybody allowed to damage their reputation or honour. Every person has a right to protection from such interference. International human rights treaties specifically recognise the right to privacy as a human right." The "ICCPR,"[3] the "ICPRAMW,"[4] and the "UNCRC"[5] all used similar phrasing. For safeguarding this privacy rights, data protection regulations are essential. Under the Information Technology Act of 2000's Section 2(1)(o), "data" is defined.It says *"a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer." The electronic consent framework issued by the Digital Locker Authority defines 'data' to mean "any electronic information that is held by a public or private service provider (like a government service department, a bank, a document repository, etc. This may include both static documents and transactional documents'. However, the concept of data is not only restricted to electronic information but also extends to information stored in physical form, e.g. on a piece of paper"*[6]

[2] Universal Declaration of Human Rights, 1948.
[3] International Covenant on Civil and Political Rights, 1966
[4] International Convention on Protection of Rights of All Migration Workers, 1990
[5] The United Nations Convention on the Rights of Child, 1989
[6] Section 2(1)(o) of the Information Technology Act of 2000

The "Indian Constitution," the "IT Act of 2000," the "Indian Contract Act," and other laws relating to intellectual property, and some others, administer data protection in India because there isn't much set of regulations therein. Recently withdrawn from consideration in parliament was the "Data Protection Bill." The Digital Personal Data Protection Bill, 2022, has now been proposed.

"Over-the-top (OTT)" digital services are webcasting content providers services that are provided to users directly over the Web. It doesn't use usual controllers or distributors of these material, like cord, broadcasting, & satellite tv systems. Additionally, it is used to refer to smartphones with out any carriers, in which all connections are priced as data, preventing monopoly power, or applications for smartphones which send data in this way, including both those that substitute conventional calling ways as well as those who refresh technology. Most widely watched OTT material is still known as over-the-top, sometimes known as online tv, web t.v, or streamed t.v. As opposed to obtaining the television signal through such a conventional transmission or satellites, the transmission is obtained over the Internet or via a mobile network. This media distributors manages accessibility using either an apps or a different OTT adapter or boxes, linked to a smartphone, Computer, or smart tv.

III. PRIVACY AND DATA PROTECTION THREATS IN OTT PLATFORMS & ITS IMPACTS

The gadget fascinated youth now favours OTT as their recreation option. Concerns to data protection and privacy also accompany such spread, that could destroy the business plan. A new Application security danger scenario, that, though not handled right, may possibly wreck the momentum, threatens its ability for expansion with in OTT industry.Some of the most significant security issues affecting the OTT structure include **"reverse engineering", "malware assaults", "data leaks", "SO file alteration", and "app forging".** By altering "**SO files** (shared object files are used to load common files into the library)", intruders attempt to gain **"unauthorized access to information"** to their subscription services to take advantage of free access to unique material. If programmers don't really employ cutting-edge countermeasures in an attack surface, then corporation's financial strategy & consumer confidence are always at danger.

Another significant challenge towards the OTT application platform is **"reverse engineering".** The software program is frequently disassembled, examined, changed, & tainted before being reassembled as a fraudulent organization by attackers. Hacker may often utilize this programme to get valuable material without ever charging the publisher any more money. Those who install the malicious program risk losing sensitive files & being exposed to a variety of security

concerns.[7]

Phishing refers to getting a desire regarding information access out of a third - party provider. This is an example of informal manipulation technique in which fraudsters trick consumers into clicking on e - mails, online messaging attachments, or sites that appear legitimate in order to obtain their account information & card details. The Guardian reported that "hackers have constructed more than 700 websites that appear just like the signup pages for Netflix and Disney+ in order to profit off the epidemic streaming boom." Such fraudulent sites tempt people to sign up for discounted memberships in exchange for name, Identities, private information, even payments.

One type of threat known as **"credential stuffing"** allows attackers to accesses user's accounts by using huge amounts of data of user credentials in conjunction with bots. The most common flaw typically leads to a "credential stuffing attack" is when users use the similar username & passwords over several apps & service. These assaults constitute ideal targets for OTT applications.

Using trial-and-error, attackers can targeting account sites using a technique known as a **"brute force attack".** In order to register new accounts by the appropriate combinations, these malicious attackers utilise automatically routed to make quite numerous attempts as they could do.

These are some of the threats in OTT platforms which tends to violate privacy and threat to data protection also.

Strategies to Mitigate Privacy and Data Protection Threats in OTT Platforms

1. **Putting the requirements of the user first:** By ensuring that factors like focused persistence tactics, rapid enrolling, & reliable payment channels enhance overall consumer engagement. Attacker is knowledgeable programmers who create flawed techniques to send customers to various payment websites. providing an authentication process on the "OTT platform" with a strong security mechanism.
2. **Protecting personal data:** Any enterprise must prioritise protecting client information with in online world. This increasing dataset is becoming more susceptible to privacy issues as even more customers sign up as well as the network expands. A major

[7] Govindraj Basatwar, "OTT Sector Has Exploded Globally And So Has Hackers' Interest In It. Learn How To Beat Hackers To Protect Your Revenue",*August 16, 2019, Last updated September 17th, 2021, By Govindraj Basatwar - Global Business Head.* https://www.appsealing.com/ott-sector-has-exploded-globally-and-so-has-hackers-interest-in-it-learn-how-to-beat-hackers-to-protect-your-revenue/

 [ISSN 2581-5369]

reputational impact could result from a business not prioritising privacy & data protection. In contrast way, adopting the proper cyberspace safety procedures & making the correct access control solutions investments would provide you an advantage over your competitors.

3. **Avoid using chatbots & specific automation:** Bots are to blame for the significant number of "credential stuffing intrusions." Accounts invasions of customer data that are particularly susceptible to assaults being typically created by attackers using malicious nodes. Utilizing may greatly assist towards lowering these hazards. Before attempting to authorize, consumers shall validate that a website is being used by a person. For instance, in "Recaptcha" examination, a chatbot and just a person could be distinguished by their mouse movement or click patterns.

4. **Put low-fantasy security measures in place:** Customers have trouble memorising complicated credentials, thus systems that validate a person's password relatively quickly & securely using trick links, biometrics, or other methods like One time pin should be introduced. Consumer data will be protected without affecting experience for users in either way.

5. **Defence against piracy:** Due to their ability to broadcast information without cost, pirate websites seem generally well-liked in the business. Its absence of a fee marketing strategy looks extra tempting then expensive streaming apps wherein consumers will required to view anything beyond the images. Informing the consumer regarding various breaching techniques & ensuring their ability to recognise authentic versus piracy websites.

IV. REGULATORY FRAMEWORK REGARDING PRIVACY AND DATA PROTECTION IN OTT PLATFORMS IN INDIA

There seems to be presently no adequate Indian law that expressly addresses "privacy and data protection in OTT" As text of the 2019 Data Protection Bill has also been dropped. In spite of the lack of a regulation, India nonetheless has laws dealing with "data protection and privacy." Constitution and statutory protection are indeed the 2 types of protections that we can see. Article 21, which is part iii of the Constitution's provision on the "right to life and personal liberty," provides the protection provided by the Constitution. It has also been recognised as a fundamental right in *Puttaswami's case.*[8]

[8] *K. S. Puttaswamy (Retd.) v Union of India, (2015) 8 SCC 735.*

The "Information Technology Act of 2000" provides statutory protection against cyberattacks and e-commerce. The above legislation is concerned about "data protection." Sections 65 & 66 of the law, for example, deal with prohibiting unauthorised use of technologies, including computers, laptops, and other devices. Section 65 of the law, which includes a penalties provision for any data description addresses anybody who knows or willfully changes, destroys, or hides any computer source code. Additionally, section 69 (A) of the aforementioned act's 2008 modification was added, giving the government authority to "prohibit, intercept, monitor, and decrypt computer systems and devices as well as to block the data they contain." The "2011 Rules for Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information)" deal with Among other things, it contains details on credit/debit card information, passwords, biometrics (such fingerprints and Deoxyribonucleic Acid), as well as issues with bodily, psychological, and physical health. Additionally, it is clearly stated in such Rules that neither content that is within the public realm and that anyone could see and get for free is to be labelled as SDP. Such Regulation specified that anybody handling, acquiring, or sharing any personally identifiable information that is sensitive to the individual should follow acceptable security requirements or processes. If some damage resulted from the breach of privacy, the corporate body could be forced to make up for this by paying the person who lost.[9] According to rule 5 of the regulations,[10] "no entity, corporation, or individual shall collect sensitive personal data or information unless it is done so for legitimate purposes and is deemed required for those objectives. The individual must be informed that their data is being collected, together with its aim, receivers, as well as the name and location of the organisation responsible for gathering it, before any data is taken from them. Other issue is the uncertainty around the length of time that the entity may keep the person's private information on file." The possibility of sharing personal data with third-parties raises one major issue.

The Central Government of India sought to broaden the "Ministry of Information and Broadcasting's" purview to include electronic media platforms, OTT movie releases, including multimedia programming produced via media companies. 2 new entry, 22A and 22B, have been added to the "Schedule 2" of the "Government of India (Allocation of Business) Rules, 1961" as a result of the notifications that was released by Secretariat on Nov. 9, 2020. “The two new entries are as follows: 1. Films and Audio Visual programmes made available by online content providers 2. News and Current Affairs on online platforms.”[11]

[9] Vijay Pal Dalmia, Advocates, “India: Data protection laws in India-Everything you must know”,available at: www.mondaq.com/India/x/655034/data+protection/Data+Protection+Laws+In+India

[10] Rule 5 of IT Rules

[11] THE GAZETTE OF INDIA : EXTRAORDINARY [PART II—SEC. 3(ii)] CG-DL-E-10112020-223032,

Online content that is now published in India is controlled like a result of such a incorporation. It comprises reports, social networks, & current events material in addition to OTT network data. Such legislation is seen to be necessary due to the huge amount of uncontrolled material which is accessible via the internet and the absence of an effective legal regime that can provide users with protections. A regulatory framework was desperately needed for OTT , more so to guarantee protection for its viewers rather than limit the rights of creatives.

A self regulatory policy which specified a list of guidelines for monitoring & forbidding 5 categories of contents was accepted by OTT service players in 2019 in anticipation of the government's involvement. These are -

1. Item which blatantly & intentionally denigrates a country's flag or symbol.
2. A representation or plot which supports "child pornography".
3. Whatever item "maliciously" aims to offend religious sensibilities.
4. Anything which "intentionally and maliciously" supports or fosters extremism.
5. Anything that is restricted by statute or perhaps by a judiciary from showing or sharing.[12]

In case of *Shashank Shekhar Jha vs Union Of India,* In a Public Interest Litigation (PIL) filed calling for regulating the Ott services by a self-governing body, "the Apex court requested the center's answer. The PIL stated that these sites, whereby digital information is made available to the public without any kind of filtration or review, were not subject toward any regulations. The government, the Ministry of Information and Broadcasting (MIB), and the Internet and Mobile Association of India were then served notice by the bench, which was made up of then Chief Justice SA Bobde, Justices AS Bopanna, and V Ramasubramanian."[13]

Concerning how will M.I.B. proposes to control digital material, very little details are available. One approach is to use the "Programme Code", which controls how programming is shown on tv channels, as a model. Other idea under consideration is to modify the "Programme Code" so that it encompasses OTT networks & digital material.

The government had released the draft of the "Digital Personal Data Protection bill". The "Digital Personal Data Protection Bill" is a piece of legislation that outlines the responsibilities and rights of the citizens on the one side as well as the duty of the "Data Fiduciary" to use

Accessed on : https://egazette.nic.in/WriteReadData/2020/223032.pdf

[12] Jidesh Kumar and Nivetha George, "India: Government Issues Regulations For OTT Platforms And Online Content", 20 November 2020. Accessed on : 4.12.2022
https://www.mondaq.com/india/broadcasting-film-tv-radio/1007904/government-issues-regulations-for-ott-platforms-and-online-content

[13] *Shashank Shekhar Jha vs Union Of India on 15 October, 2020 - Writ Petition(s)(Civil) No(s).1080/2020*

gathered data legitimately the other. Taking "necessary security procedures to avoid personal data breach, a penalty of up to Rs 200 crore would be assessed" is a requirement for any company, data custodian, or processors managing customers' personal data. However this draft bill is dealing with data protection but specifically OTT regulation is not mentioned.

Currently there is not any specific legislation which is dealing with Privacy And Data Protection In Ott Platforms. The governing agency has to provide additional information regarding its intentions to impose licences, rules, or restraints on the surveillance of OTT Platforms.

V. CONCLUSION

In this paper I have analysed the Privacy And Data Protection Issues in OTT Platforms. The meaning of Privacy And Data Protection and OTT is discussed. The paper had also discussed the concerns regarding the Privacy And Data Protection in OTT and the methods to mitigateit. Then the present regulatory framework with respect to India had been discussed. It also gives an explanation of relevant laws and court rulings.Protecting people's "data" is the goal of "data protection." This "right to privacy" has been declared to be a "fundamental right in India" as a consequence of court rulings. The IT Act, the Rules of 2011, and other laws now in effect does not specifically deals in protecting Privacy And Data Protection in OTT. The government had released the draft of the "Digital Personal Data Protection bill". However this draft bill is dealing with data protection but specifically OTT regulation is not mentioned. For OTT broadcasters & distributor both, such information is an important financial product since it helps companies quickly identify its audience. This data is later integrated with other information, such as that coming from external agencies, but might contain details about the users' personal preferences & traits. All of this data is put to use by the OTT to enhance its offerings & present pertinent, tailored upgrade chances. Hardly a company make it simple to comprehend which information will be treated about which particular goals. It is challenging to grasp & comprehend corporate confidentiality & policy frameworks regarding cookies or attention advertising. These seem difficult to understand because they're unclear in certain key areas and don't specify precisely exactly how and why individual data is utilised. People' interests & preferences are discovered to really be unpleasant to comprehend due to their hazy communication. But the ultimate issue is that internet businesses increasingly collecting excessively many users’ data. It is essential to comprehend well how to protect one's information and the amount of information businesses have about consumers as tech improves more intricately. When providing personal information, every visitor should review the privacy regulations of every service. Therefore, the administration must put in place a dependable mechanism which might alert stakeholders &

 [ISSN 2581-5369]

urge authorities to take actions as quickly as possible. Additionally, policymakers are required to enact laws, guidelines, & regulations which ensure the safety of the gathered information. A databases in which the information is stored needs to be securely safeguarded to avoid accessibility even by professionals. The mechanism for a punishment, including such imprisonment and fines must also be included in any regulation so that anyone who treats personal data inappropriately would be sufficiently punished.

*****

 [ISSN 2581-5369]