CHAPTER 4: DIGITAL RIGHTS AROUND THE WORLD

4.1 Introduction

Sharing of personal data is always seen as a danger to an individual's privacy. Many privacy and security experts will avoid using products or companies who collect their data and share it with third parties. Though, this approach is not wrong, and it does offer you a considerable amount of privacy and security when you use products which are not collecting your data and selling it to others to make profits.

Data sharing is not always bad, sometimes small companies and new start-ups can benefit from data sharing. The founders of PhonePe once said in his speech that how the open data available of the UPI made it easier for them to start a successful company.[1]

Sharing of anonymised can be useful in some particular circumstance, it might allow us to train Artificial Intelligence and Machine Learning Algorithms, etc. On the other hand, some reports say that anonymised data can be deanonymised and liked back to the originator.

In the chapter, the researcher will talk about different data protection rules in different countries, the researcher will mainly focus on European and Indian laws.

Europe's GDPR was a front-runner in data protection legislation in the world, it was a great starting point for other countries as well. Europe's GDPR was applauded as the right move in the right direction. This allowed European citizens to claim their digital rights, private companies were forced to become GDPR-compliant in order to continue doing business in Europe.[2]

At the beginning of this paper, the researcher mentioned how law and society are interlinked. Having poor data protection regulations aid companies to go to extreme and exploit user data, and make profits out of it. On the other hand, having strong data protection regulations encourages companies to make privacy-friendly products and services. Switzerland is considered to have the gold standard of data protection laws, and as a result, we see companies like Threema[3] and ProtonMail[4] having their headquarters there. Both Threema and ProtonMail are privacy respecting companies, and they develop and sell privacy-friendly technologies.

If India will have similar standards of data protection regulations, we might see more and more privacy respecting companies investing in the Indian market. Recently, CERT-IN[5] released a new regulation, asking VPN service providers to log user data, as a result a few VPN services are considering to leave Indian market.[6] If, on the other hand, India had better regulations, maybe more and more reputed VPN companies might have rushed to set up their offices in India.[7]

4.2 Legal Framework in Europe

A framework is a particular set of rules, ideas, or beliefs which you use in order to deal with problems or to decide what to do.[8] A legal framework on the other is a set of laws which we use to deal with concerns or to decide what to do.

4.2.1 General Data Protection Regulation

The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. The GDPR is an important component of EU privacy law and of human rights law.[9]

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

The right to privacy is part of the 1950 European Convention on Human Rights, which states, “Everyone has the right to respect for his private and family life, his home and his correspondence.” From this basis, the European Union has sought to ensure the protection of this right through legislation.[10]

As technology progressed and the Internet was invented, the EU recognized the need for modern protections and in 1995 it passed the European Data Protection Directive, establishing minimum data privacy and security standards, upon which each member state based its own implementing law. But already the Internet was morphing into the data hoarder it is today. In 1994, the first banner ad appeared online. In 2000, a majority of financial institutions offered online banking. In 2006, Facebook opened to the public. In 2011, a Google user sued the company for scanning her emails. Two months after that, Europe’s data protection authority declared the EU needed “a comprehensive approach on personal data protection” and work began to update the 1995 directive.

The GDPR entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant.

4.2.2 Spain

Apart from the GDPR, countries in Europe have many municipal laws governing the digital space.

For example, the right to privacy is enshrined in the Constitution of Spain. The secrecy of telephone communications is a Fundamental Right, guaranteed in the Spanish Constitution.[11]

Article 18.3 Right to intimacy. Inviolability of the home.: Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary.

No one except a judge (in the context of an investigation) may order the intervention of communications. In no case, and under no pretext, can the intervention of communications is ordered, except through a judge.

The judge is the only authority with constitutionally conferred power and responsibility to determine the appropriateness of the measure, without forgetting the protection of the rights of those who suffer it.

4.2.3 United Kingdom

In the United Kingdom, there are over 600 public authorities who can use investigatory powers. However, not every organisation can use every power. The most intrusive powers can exclusively be used by a small number.

Who can use what power is controlled by five key pieces of legislation:

1. Investigatory Powers Act 2016
2. Regulation of Investigatory Powers Act 2000
3. Regulations of Investigatory Powers (Scotland) Act 2000
4. Police Act 1997
5. Intelligence Services Act 1994

These laws give power to the authorities to infringe upon the personal liberty of the individual in a lawful manner, these laws also guide the authorities when not to interfere and protect the individual's right to personal liberty and right to privacy.

For example, the Regulation of Investigatory Powers Act 2000 makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications.

However, the interception is lawful only in the limited circumstances set out in section 1(5) of RIPA. The law also laid down the correct procedure to intercept the communication, and this will result in a serious breach of privacy of the individual, it is important to follow the correct procedure laid down by the law.

4.3 Legal Framework in India

India, the largest democracy in the world and second-largest internet user base, has been trying to enact a national data protection law for quite some time now.

The Information Technology Act, 2000, also known as the IT Act, 2000 in short, is an important legislation that is frequently referred to in the daily news.

The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce.

Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged.

The law prescribes penalties for various cybercrimes and fraud through digital/electronic format. It also gives legal recognition to digital signatures.[12]

In July 2017, the Ministry of Electronics and Information Technology set up a committee to study issues related to data protection. The committee was chaired by retired Supreme Court judge Justice B. N. Srikrishna. [13]

The committee submitted the draft Personal Data Protection Bill, 2018 in July 2018. After further deliberations the Bill was approved by the cabinet ministry of India on 4 December 2019 as the Personal Data Protection Bill, 2019 and tabled in the Lok Sabha on 11 December 2019.

The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India. Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.[14]

In India, we do not have a proper legal framework of law regarding digital rights. Compared to other countries, in the field of digital security, we have a lot of work to do.

4.3.1 Telegraph Act, 1885

Section 5 of the Telegraph Act is commonly known as the wire-tapping clause. It gives power to the government to take possession of any licensed telegraphs in case of a public emergency or in the interest of public safety. It can also order interception of communication in the interests of the sovereignty and integrity of India, the security of the state, friendly relation with foreign states or public order or for preventing incitement to the commission of an offence. However, the government has to follow the procedure established by law for issuing such order.

The procedures and guidelines for lawful interception was laid down in the case of People's Union for Civil Liberties v. Union of India (1997) 1 SCC 318.[15] In this case, the Supreme Court of India ruled that telephone tapping is a serious invasion upon an individual's privacy. However, lawful interception can be carried out under certain circumstances mentioned in the wiretapping provision. This kind of law interception has to be carried in conformity with certain guidelines, which will act as a check on indiscriminate wire-tapping by the law enforcement agencies. It also directed the government to make rules and procedures for carrying out lawful interception of communication. In addition to that, it also laid down the basic guidelines for such interception. The main guidelines are:

1. An order for law interception can only be made by the Home Secretary to the Government of India and home secretaries of state governments. In urgent situations the power may be delegated to an officer of the Home Department of the Government of India and state governments and such officer should not be below the rank of joint secretary.
2. A copy of the order has to be sent to the review committee within one week of issuance of such order.
3. The authority which issues the order should also record the following information:

- the intercepted communications;
- the extent to which the material is disclosed;
- the number of persons and their identity to whom any of the material is disclosed;
- the extent to which the material is copied; and
- the number of copies made of the materials.

4. The intercepted material can be used only for purposes mentioned under the wire-tapping clause.

5. The interception will be valid for two months unless it is renewed. However, the total period of interception should not exceed six months.

4.3.2 Information Technology Act, 2000

India's Information Technology Act is based on the Model Law on E-Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL).[16] The Act recognizes the legal validity of E-documents, E-signatures and E-contracts, and also promotes E-government. E-documents are not allowed in wills, trusts, sales of real property, negotiable instruments and powers-of-attorney.

An E-document may be used to satisfy a statutory requirement of writing; authentication; retention; publication; and governmental filing, issuance or payment. A digital signature complies with a statutory requirement for a handwritten signature to be affixed on paper.[17]

India's privacy laws are scattered among different statutes. But the Information Technology Act is the primary law concerning data protection because it addresses itself to electronic commerce.[18]

The concept of privacy differs from society to society. The concept of privacy in modern times is not restricted to mere physical movement or domiciliary surveillance, but also encompasses protection of a wide range of information, whether it's medical, financial, biometric or personal etc.[19]

India does not have specific legislation to deal with issues of privacy, however the Information Technology Act 2000 provides protection in the form of damages in case of failure to protect data and criminal liability in case of wrongful disclosure of information in breach of a lawful contract. Protection of data is an important concern as it protects one's right to privacy, further stolen data can be a matter for concern as it can be misused for personal gain and to cause loss to another person. This paper deals with Privacy and the Information Technology Act, 2000 as there is no specified legislation to deal with Privacy.[20]

India presently does not have any express legislation governing data protection or privacy. However, the relevant laws in India dealing with data protection are the Information Technology Act, 2000 and the Indian Contract Act, 1872. A codified law on the subject of data protection is likely to be introduced in India in the near future.[21]

The Indian Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Under section 43A of the Indian Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then

such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

Section 43A: Compensation for failure to protect data.

Under section 72A of the Indian Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

Section 72A: Punishment for disclosure of information in breach of lawful contract.

1. Criticisms of Information Technology Act, 2000

Accountability. The first criticism of India's IT Act 2000 was directed at accountability. The IT Act did not impose liability on companies themselves even when they bore the ultimate responsibility for protecting personal data. Instead only those individuals who directly violated the IT Act could be prosecuted. Thus if a company left customer data on an unsecured, publicly accessible server through sheer negligence, only those who accessed and stole data from the server could be prosecuted. As it turns out, that criticism was only partly true. It concerned IT Act section 85, which I will discuss below.

No data-breach notification. For business and e-commerce purposes, what is needed are data-breach notification provisions. When a company becomes aware, or when it should be aware, of unauthorized access to personal information, it must notify the individual whose information was accessed. In the United States, 46 states have implemented data-breach notification laws.[22] To comply with those states' laws, U.S. companies must require data-breach notification in their outsourcing contracts with Indian service providers.

Purpose Specification and Use Limitation. The IT Act does not impose limits on the collection of personal data and proper use of that data. Privacy groups and organizations have long insisted that companies give fair notice to consumers when personal data is being collected and what it will be used for. If the data will be used for purposes beyond what was originally requested, companies must request separate permission for those new purposes.[23]

2. A Way Forward

The Information Technology Act, 2000 is not data or privacy protection legislation per se. It does not lay down any specific data protection or privacy principles. The Information Technology Act, 2000 is a generic legislation, which articulates on range of themes, like digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. It suffers from a one Act syndrome.[24]

In fact, the Information Technology Act, 2000 deals with the issue of data protection and privacy in a piecemeal fashion. There is no an actual legal framework in the form of Data Protection Authority, data quality and proportionality, data transparency etc. which properly addresses and covers data protection

issues. Even if the new proposed amendments to the Information Technology Act, 2000 were adopted, India would still lack a real legal framework for data protection and privacy.[25]

4.3.3 Personal Data Protection Bill, 2019

The 2019 Bill is broadly based on the principles of the General Data Protection Regulation, 2016 (the "GDPR") and the landmark judgment of the Supreme Court of India: Justice K.S. Puttaswamy (Retd.) & Anr vs Union of India, W.P. (Civil) No. 494 of 2012), wherein right to privacy was upheld as a fundamental right under the Indian Constitution. [26]

The 2019 Bill intends to protect the privacy rights of individuals with respect to their personal data and governs and regulates the organizations processing such personal data.

This Bill is applicable to the whole of India, any entity located in India and only processing personal data of foreign nationals not present in India may be exempted from the application of the Bill by the Central Government.

1. Definition of Personal Data

Under the 2018 Bill, personal data has had been defined to mean "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information." [27]

The definition of 'personal data' under the 2019 Bill has been considerably broadened to read as "personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include inference drawn from such data for the purpose of profiling." [28]

Data which can be used to identify you is called personal data. For example, information about you, name, age, birth place, sex, banking details, social media user names, browsing behavior, location data, bio-metric data, etc can be classified as personal data.

Companies usually collect anonymized data about you to improve their services. Recent reports suggests, that anonymized data can also be used to identify you, hence they are not really anonymous.

Data mining companies like Google and Facebook collect all types of data about you to serve ads. These kinds of practices are not illegal as you consent to these companies to collect your data by agreeing to their privacy policy and terms of use.

The Personal Data Protection Bill, 2019 is a Bill to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals

2. Analytical School Of Jurisprudence

The major premises of analytical school of jurisprudence is to deal with law as it exists in the present form. They treat law as a command emanating from the Sovereign, namely, the state.[29]

By this, the Personal Data Protection Bill, 2019 will be a good law, as it will be a command of the sovereign.

However, Jeremy Bentham, a famous jurist from the analytical school of jurisprudence have a different opinion regarding the concept of a good law.

3. Bentham's Theory of Utilitarianism

Bentham in his theory of Utilitarianism said, that the right aim of a legislation is to carry out the principle of unity. In other words, the proper end of every law is to promote the greatest happiness of the greatest number of people.[30]

The task of the government is to promote the happiness of the society, by furthering the enjoyment of pleasure and minimizing the pain

Is the Personal Data Protection Bill, 2019 a good law, if we live in a utilitarian society?

To answer this, let us understand this Bill and try to figure out what amount of pleasure or pain we can derive from it.

4. Data Protection Principles and Rights

The PDP Bill, 2019 provide some user rights, including the rights to confirmation and access, the right to correction and erasure, and the right to data portability. The right to erasure has been added from the previous iteration of the PDP Bill, and is a welcome step.[31]

The Bill also provides a right to information, does not contain the right to an explanation like in the EU's GDPR or UK's Data Protection Act, 2018.

It is limited to a "brief summary" of the personal data being processed and the processing activities.

"We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos." [32]

This is from Google's privacy policy, these 42 words explain that everything you do on Google, from using their search engine or YouTube, to saving your private photos and documents in Google Drive, etc are being collected by Google. Your emails are not that private as you think, everything you type is being collected by google. Google knows that I copied a paragraph from their privacy policy.

5. How do Google use all the collected data about you?

“We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you’ll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.” [33]

Only 71 words to explain how they use your data. If you need to know more the right to explanation comes handy, the right to explanation is crucial for accountability and transparency in the use of algorithms to make decisions in our lives.

For utilitarianism, this new right gives the user lot of freedom, which will help them to decide whether to make a new account on Google or not. No pain, only pure pleasure to the people.

6. Establish a strong and independent data protection authority, and appellate tribunal

No comprehensive data protection framework can be effective without a dynamic and powerful enforcement mechanism. A powerful enforcement mechanism includes the creation of an independent data protection authority.[34]

Clause 41 of the PDP Bill seeks to establish and incorporate a data protection authority for the purposes of the PDP Bill, which will be known as the Data Protection Authority of India. As per the current text of the PDP Bill, the chairperson and the members of the Authority shall be decided by a committee of six members, consisting members from the executive branch of the State.

The criteria for membership provided under the PDP Bill is vague, and given that the appointments are made by the government, there is a possibility of a pro-government bias creeping into the Authority.

In India, the government may soon be the biggest processor of data. This proposed nomination process raises concerns regarding the independence of the Authority and requires considerable improvement; the government’s modifications of the original text proposed by the Srikrishna Committee has actually weakened the independence of the Authority.

Worlds most privacy conscious companies and organizations prefer to be incorporated in Switzerland, or host their servers in Switzerland. Why Switzerland? That country has a great reputation of having strong privacy laws. Hence, every major privacy focused company or organization chooses Switzerland. [35]

Strong privacy laws in India will surely attract more privacy focused organizations into India, hence, increasing job opportunities for the Indians at the same time it will also protect the worlds largest democracy’s citizens’ personal data.

Every major security and privacy focused organization are usually open sourced and have a third party security audit. Organizations like Signal, ProtonMail[36], etc 100% open sourced and are audited for security flaws and back-doors by third party auditors.

From this we know that these organizations are not indulging in malpractices which will compromise users personal data.

Comparing this to the Data Protection Authority, which is neither independent in its nature nor complete free from external influences lie from the government is not a good step to achieve industrial standards of complete user privacy and data security.

7. Strengthen the provisions regarding reporting of data breaches by data fiduciaries

Clause 25 of the PDP Bill provides for a legal requirement for data fiduciaries to inform the Data Protection Authority (Authority) of breaches of personal data.[37]

In case of a data breach, the data fiduciary has to notify the Authority regarding the breach, where such breach is likely to cause harm to any data principal. The notification sent to the Authority is supposed to include details on the nature of personal data, number of data principals affected, possible consequences, and measures being taken by the data fiduciary.

Further, informing the data principal about the breach depends on the discretion of the Authority.

There are services online like ‘Have I Been Pawned?’ which can inform you if your email address have been a part of a major reported data breach. [38]

As mentioned above, even the anonymized data can be used to identify an individual, any sort of data breach can be harmful. But data breaches of personal data are more harmful.

21st Century have been a century of data breaches. We have seen number of data breaches from Facebook’s Cambridge Analytical[39] to Marriott International's guest list data being compromised. [40]

As a user of a service, it is of my utmost importance to have a good user experience, if the service inform me of any data breach compromising my data. Google informs its users about compromised passwords, Firefox informs its users about compromised emails. Data breaches are dangerous because data is the new oil, leaked data is soled to advertisers, criminals, scammers, etc.

The clause that the Authority has the discretion whether to inform the data principle about the breach is unreasonable. Every single data breach must be informed to the data principle. User reporting should instead by the default.

Limiting the scope of Clause 25 will only increase the amount of pain and damage suffered by the society.

8. Processing of personal data without the consent of the data principal

Clause 11 of the Bill says that anyone’s personal data shall not be processed, except on the consent given by the data principal.[41]

The term ‘data principle’ have been defined under Clause 3 (14) of the Bill as, “the natural person to whom the personal data relates.”

However, in Chapter 3 of the Bill, which is concerned with the grounds for processing of personal data without consent is an exception to the Clause 11 of the Bill.

The state is authorized to process personal data for "the exercise of any function of the state" without the consent of the individual. The provision is vague and over broad, and it gives the government an absolute power over citizens' data and rights. It is imperative that data protection principles apply to the state as well as to private actors. Further, the processing of personal data to comply with any law, order, or judgment of courts or tribunals, is allowed without the need for the consent of the data principal. These provisions are particularly harmful.

Further, in addition to the exemptions above, Clause 12(f) provides an exception wherein processing of personal data may be done without any consent of the users, in case of "breakdown of public order". Such broad, undefined language, especially in the background of deployment of mass facial recognition and other technologies, creates concern, and may lead to the mass surveillance of users.

The aim of this legislation is to establish users' protection and it should not be turned as a tool to justify the deployment of techniques and technologies that enable surveillance.

Clause 14 allows an exception where personal data may be processed without consent for "reasonable purposes". This phrase is vague and gives latitude for violating the data rights of citizens. The presence of an illustrative list of "reasonable purposes" is concerned as it seeks to include "credit scoring", "recovery of debt", etc., already indicating that "reasonable" commercial interests could trump rights-protecting data protection measures.

9. Risk of mass surveillance and other privacy harms

In addition to the exemptions provided for the processing of data without the consent of the data principal, Clause 35 of the PDP Bill provides broad provisions under which the government can exempt its own departments from the very application of the law itself.[42]

These exemptions are too vague and dangerously broad. As noted by many experts, there is a need for the tightening and evolution of Indian statutory law overseeing the processing, including collection and use of data by government agencies - including those engaged in law enforcement matters and other areas of internal security and intelligence. The absence of comprehensive surveillance law reform provides the State with wide access powers over the information of citizens of India, and thus puts their informational privacy under threat. This contradicts the spirit and aim of the PDP Bill.

10. Transfer of sensitive personal data and critical personal data outside India

The PDP Bill tries to establish a data localization regime. Data localization means that the data of the Indian users will be stored locally subject to Indian jurisdiction. Clause 33 of the PDP Bill allows for sensitive personal data to be transferred outside India by a data fiduciary with the consent of the data principle. [43] But this Clause makes it mandatory that such sensitive personal data shall be continued to be stored in India.

Given this context of the lack of sufficient curbs on access to such data by the government in India, this proposed data localization provision betrays a governmental interest in desiring more control over the data of Indian citizens - not protecting privacy. However, there is one benefit to data localization, that is, it will increase the speed of the internet, as now the data is being stored physically closer to the user in servers situated in India.

On the other hand, all sensitive personal data will be stored in India. Personal data is any data which can identify you. Sensitive personal data is data which contains sensitive information about you, like sexual orientation, religion, passwords, health insurance, etc. If this personal data falls in the wrong hands, this can be used against you. Moreover, when sensitive personal data is stored in India, it will make mass surveillance easier on the citizens of India. I would rather prefer to have my personal data stored somewhere under Swizz jurisdiction than under Indian jurisdiction. Not only there is a threat of mass surveillance and a chance India becoming an Orwellian regime. [44]

In history, Indian government had soled details of Indian drivers' licence holders to private companies. The government is supposed to be our best friend, not a big brother. The Personal Data Protection Bill, 2019 is a good law as the idea of data localization will increase the internet speed. But this increase of speed will not be very significant. The Personal Data Protection Bill, 2019 is a bad law as it will make India an Orwellian State.

Privacy matters. Right to privacy is a human right, right to privacy is our fundamental right.

Privacy matters because; [45]

- It protects our property.
- It helps to protect our beliefs.
- It helps protect our nationality.
- It helps to protect us from persecution.
- It protects our ability to move freely.
- It protects our freedom to choice.
- It facilitates our access to justice.
- It ensures we are all recognized people.
- It can protect us from torture.
- It is about being free.
- It can protect our lives.
- It can protect us from discrimination.

Is it really justified to invade some ones privacy for national security?

This is a debate between security vs privacy. The people are not divided on the two extremes, majority thinks that a reasonable encroachment to users privacy is justified only if it's making our nation safer.

However, in reality this is not the case. Governments do spy on its own citizens mainly for their own gain. For example, to suppress dissent, protests, to dig dirt on the opposition.

But what about terrorist attacks? After 9/11 the National Security Agency of the USA took the surveillance program to another level.

And now USA is the safest country to live in? No, it is not.

The White House appointed two independent commissions after Snowden's revelation in 2013 to review mass surveillance programs. Do these have any value? Should they be changed? Should they be reformed?

Those commissions looked at the classified evidence and they found, despite the fact the these mass surveillance programs are being going on since 2001, it had never stopped a single terrorist attack in USA. And both of them found that these programs should be ended. [46]

Currently the Indian surveillance laws give the Indian government a lot of power to spy on its own citizens to protect national security.

Even after all this, the Indian security agency was not able to prevent the Pulwama attack back in 2018.

The government with the help of an Israeli security firm managed to target many activists and journalists for their own gain, not for the country's gain.

21st Century is the beginning of mass surveillance worldwide, it will only get worst in the future. To stop this we all need to unite and fight for our privacy. We need to find alternatives to mass surveillance to fight terrorism and to maintain national security.

Why don't the people care about this already? Part of it is because it happened invisibly.

4.3.4 Information Technology (Guidelines For Intermediaries And Digital Media Ethics Code) Rules, 2021

1. About the Rules

The Rules prescribe a framework for the regulation of content by online publishers of news and current affairs content, and curated audiovisual content.

Social media intermediaries, with registered users in India above a notified threshold, have been classified as significant social media intermediaries (SSMIs). SSMIs are required to observe certain additional due diligence such as appointing certain personnel for compliance, enabling identification of the first originator of the information on its platform under certain conditions, and deploying technology-based measures on a best-effort basis to identify certain types of content.

All intermediaries are required to provide a grievance redressal mechanism for resolving complaints from users or victims. A three-tier grievance redressal mechanism with varying levels of self-regulation has been prescribed for publishers.

2. Definitions

Rule 2 is the definition clause. For our purposes, the following definitions are important:

Rule 2(v) defines a significant social media intermediary as one being above a certain threshold which may be notified by the Central government, (the user limit for this has been set at fifty lakhs and above)

Rule 2(w) defines a social media intermediary as one which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.

3. Key Features

A. Due diligence by intermediaries: Under the IT Act, an intermediary is not liable for the third-party information that it holds or transmits. However, to claim such exemption, it must adhere to the due diligence requirements under the IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (which replace the earlier 2011 Rules). Under the 2011 Rules, the requirements included: (i) specifying, in service agreements, the categories of content that users are not allowed to upload or share, (ii) taking down content within 36 hours of receiving a court or government order, (iii) assisting law enforcement agencies, (iv) retaining blocked content and associated records for 90 days, and (v) providing a grievance redressal mechanism for users and affected persons, and designating a grievance officer. The 2021 Rules retain these requirements, while: (i) modifying the categories of content that users are not allowed to upload or share, and (ii) prescribing stricter timelines for the above requirements.[47]

B. Significant social media intermediaries: The 2021 Rules define social media intermediaries as intermediaries which primarily or solely enable online interaction between two or more users. Intermediaries with registered users above a notified threshold will be classified as significant social media intermediaries (SSMIs). The additional due diligence to be observed by these SSMIs include:

Personnel**:** An SSMI must appoint: (i) a chief compliance officer for ensuring compliance with the Rules and the Act, (ii) a nodal person for coordination with law enforcement agencies, and (iii) a grievance officer, all of whom should reside in India.

Identifying the first originator of information**:** An SSMI, which primarily provides messaging services, must enable the identification of the first originator of information within India on its platform. This may be required by an order of a Court or the competent authority under the IT Act. Such orders will be issued on specified grounds including prevention, detection, and investigation of certain offences such as those relating to national security, public order, and sexual violence. Such orders will not be issued if the originator could be identified by less intrusive means.

Technology-based measures: SSMIs will endeavour to deploy technology-based measures to identify: (i) content depicting child sexual abuse and rape, or (ii) information that is identical to the information previously blocked upon a court or government order. Such measures: (i) must be proportionate to interests of free speech and privacy of users, and (ii) have a human oversight and be reviewed periodically.

User-centric requirements**:** SSMIs must provide users with: (i) a voluntary identity verification mechanism, (ii) a mechanism to check the status of grievances, (iii) an explanation if no action is taken on a complaint, and (iv) a notice where the SSMI blocks the user's content on its own accord, with a dispute resolution mechanism.

C. Digital Media Publishers: The 2021 Rules prescribe certain requirements for online publishers of: (i) news and current affairs content which include online papers, news portals, aggregators and agencies; and (ii) curated audio-visual content, which is defined as a curated catalogue of audio-visual content (excluding news and current affairs) which is owned by, licensed by, or contracted to be transmitted by publishers and available on demand. The Rules institute a three-tier structure for regulating these publishers: (i) self-regulation by publishers, (ii) self-regulation by associations of publishers, and (iii) oversight by the central government.

D. Code of Ethics: For publishers of news and current affairs, the following existing codes will apply: (i) norms of journalistic conduct formulated by the Press Council of India, and (ii) programme code under the Cable Television Networks Regulation Act, 1995. For online publishers of curated content, the Rules prescribe the code of ethics. This code requires the publishers to: (i) classify content in specified age-appropriate categories, restrict access of age-inappropriate content by children, and implement an age verification mechanism, (ii) exercise due discretion in featuring content affecting the sovereignty and integrity of India, national security, and likely to disturb public order, (iii) consider India's multiple races and religions before featuring their beliefs and practices, and (iv) make content more accessible to disabled persons.[48]

E. Grievance redressal: Any person aggrieved by the content of a publisher may file a complaint with the publisher, who must address it within 15 days. If the person is not satisfied with the resolution, or the complaint is not addressed within the specified time, the person may escalate the complaint to the association of publishers, who must also address the complaint within 15 days. The complaint will be considered by an inter-departmental committee constituted by the Ministry of Information and Broadcasting if: (i) escalated by the complainant or the association under certain conditions, or (ii) referred by the Ministry itself.

F. Oversight by Ministry: The Ministry of Information and Broadcasting will: (i) publish a charter for self-regulating bodies, including Codes of Practices, (ii) issue appropriate advisories and orders to publishers; (iii) have powers to block content on an emergency basis (subject to review by the inter-departmental committee). Any directions for blocking content will be reviewed by a committee headed by the Cabinet Secretary.

4. Key Issues And Analysis

A. Regulation of online intermediaries.

Intermediaries include a vast array of entities who facilitate the flow of data on internet. These include telecom service providers, internet service providers, search engines, online marketplaces, payment sites, cyber cafes, messaging services, and social media sites. While many intermediaries are mere conduits or storage providers, where they are unaware of the content being transmitted or stored on their platform, other intermediaries may be aware of the user-generated content on their platform. This raises the question that to what extent intermediaries should be held liable for the user-generated content on their platform.

In some jurisdictions such as European Union and India, intermediaries are regulated through the safe harbour model. Under this model, intermediaries are granted immunity from any liability for any illegal user-generated content provided they comply with certain requirements.[49] [50] [51] The intermediaries remain immune from liability unless they are aware of the illegality and are not acting adequately to stop it.[13] They are subject to 'duties of care' and 'notice and take down' obligations to remove illegal content.

In recent years, some online platforms have gained a central role in enabling access, facilitating the exchange of information and sharing of information at scale.[52] Many online platforms have expanded their role from mere hosts of information to that of entities governing how content is displayed and shared online, and undertaking significant actions in the areas of moderation, curation, and recommendation. There are growing concerns around misuse of these platforms for the proliferation of illegal or harmful content such as child sex abuse material, content provoking terrorism, misinformation, hate speech, and voter manipulation.[53] This has raised questions on the role and responsibility of platforms in preventing diffusion, detection, and subsequent removal of such content.

Some platforms have been self-regulating the publication of such content. However, this has raised concerns about arbitrary actions taken by these platforms which could affect freedom of speech and expression. These developments pose an important challenge for the regulatory framework for intermediaries in terms of finding the correct balance between enhancing the role of platforms and governments in detection, moderation, and curation, and protection of individual's rights. The 2021 Rules may address some of these issues. Implications of certain provisions under the Rules are discussed in the following sections.

B. The Rules may be going beyond the powers delegated under the Act.

The central government has framed the 2021 Rules as per the following rule-making powers under the Act: (i) carrying out provisions of the Act, (ii) specifying the safeguards or procedures for blocking information for access by the public, and (iii) specifying due diligence to be observed by intermediaries for exemption from liability for third-party information. The 2021 Rules define new types of entities, state their obligations, and prescribe a new regulatory framework for some of these entities. This may be going beyond the powers delegated to the Executive under the Act. Such instances are discussed below. In various judgements, the Supreme Court has held that Rules cannot alter the scope, or provisions, or principles of the enabling Act.[54] [55] [56]

Distinct obligations for new classes of intermediaries: The Act defines an intermediary and states its obligations. These include:

(i) taking down content upon a court or government order,

(ii) retaining certain information,

(iii) providing information and assistance to law enforcement agencies in certain conditions, and

(iv) observing due diligence to be exempt from intermediary liability.

The Rules define two new classes of intermediaries: (i) social media intermediary and (ii) significant social media intermediary (SSMIs). The Rules also specify the additional due diligence to be observed by SSMIs. These include: (i) appointing certain personnel, (ii) identifying the first originator of information (where SSMIs primarily provide messaging services), and (iii) deploying technology-based measures to pro-actively

identify certain types of information on a best-effort basis.

The Rules also empower the central government to: (i) determine the threshold for classification as SSMIs, (ii) require any other intermediary to comply with additional due diligence requirements for SSMIs.

Defining new types of intermediaries, and empowering the government to specify thresholds under these definitions and cast obligations on select entities, may be going beyond the powers delegated to the government under the Act. Provisions such as the definition of new entities and their obligations may have to be specified in the parent Act.

Identification of the first originator of information: The Rules require SSMIs, which provide a service primarily or solely in the nature of messaging, to enable the identification of the first originator of information within India on its platform. This rule has no related provision under the parent Act. The Rules also prescribe certain details such as: (i) information on the first originator can be required only by a government or court order, (ii) the grounds on which such orders can be passed, and (iii) not issuing such an order if less intrusive means to obtain the information are available. It may be questioned whether this amounts to instituting legislative policy, and hence, is required to be provided in the parent Act.

Regulation of online publishers: The Rules prescribe a regulatory framework for online publishers of news and current affairs and curated audio-visual content (such as films, series, and podcast). Regulation of such publishers may be beyond the scope of the IT Act.[57]

C. Certain grounds for restricting content may affect freedom of speech.

The Constitution allows for certain reasonable restrictions with respect to freedom of speech and expression on grounds such as national security, public order, decency, and morality.[58] The IT Act prohibits uploading or sharing content which is obscene, sexually explicit, relates to child sex abuse, or violates a person's privacy.[59] The 2021 Rules specify certain additional restrictions on the types of information users of intermediary platforms can create, upload, or share. These include: (i) "harmful to child", (ii) "insulting on the basis of gender", and (iii) "knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact". Some of these restrictions are subjective and overbroad, and may adversely affect the freedom of speech and expression of users of intermediary platforms.

The Supreme Court (2015) has held that a restriction on speech, in order to be reasonable, must be narrowly tailored so as to restrict only what is absolutely necessary.[60] It also held that a speech can be limited on the grounds under the Constitution when it reaches the level of incitement. Other forms of speech even if offensive or unpopular remain protected under the Constitution.

The Rules require the intermediaries to make these restrictions part of their service agreement with users. This implies that users must exercise prior restraint, and intermediaries may interpret and decide upon the lawfulness of content on these grounds. Such over broad grounds under the Rules may not give a person clarity on what is restricted and may create a 'chilling effect' on their freedom of speech and expression. This may also lead to over-compliance from intermediaries as their exemption from liability is contingent upon observing due diligence.

While examining the 2011 Rules on intermediary guidelines, the Lok Sabha Committee on Subordinate Legislation (2013) had observed that to remove any ambiguity, the definitions of the grounds used in the

Rules should be incorporated in the Rules, if the definitions exist in other laws. If not defined in other laws, such grounds should be defined and incorporated in the Rules to ensure that no new category of crimes or offences is created through delegated legislation. The 2021 Rules do not provide definitions or references for the terms listed above and hence, may cause ambiguity regarding the interpretation of these terms.

D. Procedure for information requests from government agencies lacks safeguards.

The Rules require intermediaries to provide information under their control or possession upon request by a government agency. The government agency which is lawfully authorised for investigative or protective or cybersecurity activities may place such a request. The request may be placed for verification of identity, or prevention, detection, investigation, or prosecution of offences under any law or for cybersecurity incidents. However, the Rules do not state any procedural safeguards or requirements for such actions.

An earlier set of Rules notified in 2009 specify the procedure and safeguards subject to which interception, monitoring or decryption of information of intermediaries may be undertaken.[61] These state that such orders must be given by the union or state home secretary (with exceptions in case of unavoidable circumstances and remote regions), and be subject to review by a committee (headed by cabinet secretary or the state's chief secretary). Further, the authority issuing such orders should first consider alternate means of acquiring information.[62]

Further, the 2021 Rules do not restrict the extent or type of information that may be sought. For example, the information sought may be personal data of individuals such as details about their interaction with others. Such powers, without adequate safeguards, as those in the 2009 Rules, may adversely affect the privacy of individuals.

E. Enabling traceability may adversely affect the privacy of individuals.

The Rules require significant social media intermediaries, which provide services primarily or solely in the nature of messaging, to enable the identification of the first originator of information within India (commonly referred to as traceability). The Rules state that: (i) such identification should be required by a court order or an order passed by a competent authority under the 2009 Rules (union or state home secretary), (ii) order for identification will be passed for specified purposes including prevention, detection, and investigation of offences related to sovereignty and security of the state, public order, and sexual violence (rape, sexually explicit material or child sex abuse material), and (iii) no such order will be passed if less intrusive means are effective for the required identification.[63]

Enabling such identification may lower the degree of privacy of communication for all users. Identifying the first originator of information on a messaging platform will require the service provider to permanently store certain additional information: (i) who all exchanged a message, and (ii) the exact message or certain details which uniquely describe a message so that information in question may be matched against it. This will be required for every message exchanged over the service provider's platform to enable tracing the first originator of any message. Note that permanently storing such details about a message is not a technological necessity for providing messaging services over internet. The Rules also do not specify any timeline in terms of how far back in time the messaging service will be required to check for determining the first originator. Overall, this requirement will lead to the retention of more personal data by messaging services which goes against the principle of data minimisation. Data minimisation means limiting data collection to what is necessary to fulfil a specific purpose of data processing, and has been recognised as an important principle for the protection of personal privacy.[64] [65]

The Supreme Court (2017) has held that any infringement of the right to privacy should be proportionate to the need for such interference.[66] Traceability is required to prevent, detect, and investigate specified offences. For enabling traceability for a few messages that may be required for investigative purposes, the degree of privacy of communication of all users of online messaging services will need to be permanently lowered. Hence, the question is whether this action could be considered proportionate to the objective.

Note that a case related to the issue of traceability is currently pending before the Supreme Court.[67]

F. Framework for regulation of content of online publishers.

Content on conventional media including print, TV, film, and radio are regulated under specific laws as well as license agreements (in the case of TV and radio). These regulations seek to ensure that community standards are reflected in content easily accessible by the public. They also seek to restrict access to certain content based on its age-appropriateness and if it may be deemed unlawful.[68] Economic costs and certain licence requirements for some of these operations mean that their numbers are few. In the past few years, internet has become a more mainstream medium for the publication of news as well as entertainment content. The regulatory framework for content on digital media may not be similar to conventional media as there are certain challenges in terms of: (i) defining who is a publisher; individuals and businesses publishing online may not be regulated in the same manner, (ii) the volume of content to regulate, and (iii) enforcement (cross-border nature of internet means that publishers need not have a physical presence in India). The 2021 Rules under the IT Act prescribe a framework for regulation of content by online publishers of news and current affairs and curated audio-visual content (such as films, series, and podcasts). Certain issues with these Rules are discussed below.

G. Regulation of online publishers under the 2021 Rules may be beyond the scope of the parent Act.

The framework provides for norms and oversight mechanism for the regulation of content of online publishers. The press note by the central government on 2021 Rules noted that online publishers are digital platforms which are governed by the IT Act.6 The IT Act is aimed at providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, and to facilitate electronic filing of documents.[69] The Act prohibits cybercrime including publishing specified content such as sexually explicit content, child sex abuse material, and content violating other's privacy.[70]

Laws such as the Press Council Act, 1978, the Press and Registration of Books Act, 1867, the Cable Television Networks (Regulation) Act, 1995, and the Cinematograph Act, 1952 are specific laws regulating publishers of news in print, television broadcast of news and audio-visual content, and films, respectively (similar content through other media). Regulation of content of these classes of publishers deals with questions of freedom of press and freedom of artistic expression. It may be questioned whether regulation of online publishers is envisaged under the IT Act and hence, if the 2021 Rules exceed the scope of the Act in this regard.[71]

H. Oversight mechanism for digital news media lacks the independence accorded to print news.

The oversight mechanism for content regulation in case of news in print is under the Press Council of India (PCI), which is an independent statutory body. One of the main objectives of the PCI is to uphold the freedom of the press. The Council consists of a chairman and 28 other members including working

journalists, persons from the management of newspapers, members of Parliament, and domain experts. The Chairman is selected by the Speaker of the Lok Sabha, the Chairman of the Rajya Sabha and a member elected by the PCI. Key functions of the PCI include: (ii) adjudicating upon complaints of violation of standards, (iii) issuing directions upon violation of code of conduct including admonishing, warning, and censuring. For similar functions in case of digital news media, the oversight mechanism will be under the Ministry of Information and Broadcasting. Thus, the oversight mechanism for digital news is not through an independent statutory body unlike that for print publications.

Note that the content of TV news is regulated under the Cable Television Networks (Regulation) Act, 1995 (CTN Act).29 The CTN Act empowers the central government to prescribe programme code and advertising code to be followed by the publishers. The central government may prohibit the transmission of a programme in the public interest on certain specified grounds if it violates these codes. A three-tier self-regulation mechanism for TV broadcasters, similar to that for online publishers, has been prescribed under the CTN Act in June 2021.

I. The procedure for emergency blocking of content of online publishers lacks certain safeguards.

As per the Rules, the Secretary of the Ministry of Information and Broadcasting may pass an order for blocking the content of an online publisher in case of emergency. Such orders may be passed on certain specified grounds including national security and public order, without giving the publisher an opportunity of hearing. Such an order will be examined by the inter-departmental committee for its recommendation on the confirmation or revocation of the order. The Rules do not give the publisher an opportunity for hearing during this entire process. This is in contrast with the process for examination of violation of the code of ethics. Under this process, the concerned publisher will be allowed to appear and submit their reply and clarifications before the committee.

J. Definition of social media intermediary may be too broad.

The Rules define a social media intermediary as an intermediary which primarily or solely enables interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services. This definition may include any intermediary that enables interaction among its users. This could include email service providers, e-commerce platforms, video conferencing platforms, and internet telephony service providers.[72]

> *Privacy is a sensitive matter, under no circumstances it should be exposed to third parties without the consent of the actual owner of that personal data.*

Endnotes:

1“Regulating Non-Personal Data”, Medianama. YouTube. https://www.youtube.com/watch?v=A8vUHzNokRQ Last Accessed on 9 May 2022.

[2]"Complete Guide to GDPR Compliance", GDPR. https://gdpr.eu Last Accessed on 9 May 2022.

[3]"Threema". https://threema.ch/en Last Accessed on 9 May 2022.

[4]"Why Protonmail Is in Switzerland? An Analysis of Swiss Privacy Laws." *ProtonMail Blog*, 25 Mar. 2020, protonmail.com/blog/switzerland/. (Last visited on 22 April, 2022).

[5]On April 28, 2022, the Indian Computer Emergency Response Team (CERT-In) issued fresh directions (No. 20(3)/2022-CERT-In) under section 70B of the Information Technology (IT) Act, 2000 in relation to the information security practices, procedure, prevention, response, and reporting of cyber incidents. Issued without public consultations, these directions raise serious concerns related to state sponsored surveillance and data retention beyond need or purpose.

[6]"CERT-In Directions on Cybersecurity: An Explainer", Internet Freedom Foundation. https://internetfreedom.in/cert-in-guidelines-on-cybersecurity-an-explainer/ Last Accessed on 9 May 2022.

[7]"NordVPN Considering Exiting India Following Government Ruling on Data Sharing", IGN India. https://in.ign.com/india/171975/news/nordvpn-considering-exiting-india-following-government-ruling-on-data-sharing Last Accessed on 9 May 2022.

[8]Definition of Legal Framework, Collins Dictionary. https://www.collinsdictionary.com/dictionary/english/legal-framework Last Accessed on 5 April 2022.

[9]Europe's General Data Protection Regulation, 2018. https://gdpr.eu/ Last Accessed on 5 April 2022.

[10]"European Convention on Human Rights", European Court of Human Rights, Council of Europe. https://www.echr.coe.int/Documents/Convention_ENG.pdf Last Accessed on 5 April 2022.

[11]Constitution of Spain, Article 18(3) Secret of communications. https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf Last Accessed on 5 April 2022.

[12]Information Technology Act, 2000. https://byjus.com/free-ias-prep/information-technology-act-2000/ Last Accessed on 5 April 2022.

[13]"The Personal Data Protection Bill, 2019." PRSIndia, 24 Mar. 2020, www.prsindia.org/billtrack/personal-data-protection-bill-2019. Last visited on 22 April, 2022.

14PRS India, “The Personal Data Protection Bill, 2019”, PRS Legislative Research. https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 Last Accessed on 5 April 2022.

15People's Union of Civil Liberties (PUCL) v. Union of India. Global Freedom of Expression. (2021, July 6). https://globalfreedomofexpression.columbia.edu/cases/peoples-union-of-civil-liberties-pucl-v-union-of-india/ Last Accessed on April 26, 2022.

16Basu, S., & Jones, R. (2005). Indian Information and Technology Act 2000: review of the regulatory powers under the Act. *International Review of Law, Computers & Technology*, *19*(2), 209-230.

17Blythe, S. E. (2006). A critique of India's Information Technology Act and recommendations for improvement. *Syracuse J. Int'l L. & Com.*, *34*, 1.

18Wilson, Benjamin, Data Privacy in India: The Information Technology Act (June 1, 2010). Available at SSRN: https://ssrn.com/abstract=3323479 Last Accessed on May 21, 2022.

19RUBAVARSHINI, R. R. NANDIGA. (2017). PRIVACY AND THE INFORMATION TECHNOLOGY ACT,2000. International Journal in Management and Social Science, 5(8), 246–249.

20Rubavarshini, R. R. (2017). Privacy and the information technology act, 2000. *International Journal in Management & Social Science*, *5*(8), 246-249.

21Dalmia, V. P. (2017, December 13). Data Protection Laws in India - Everything You Must Know - Data Protection - India. Retrieved May 2, 2022, from https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know Last Accessed on May 26, 2022.

22National Conference of State Legislatures, State Security Breach Notification Laws, April 12, 2010, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLa ws/tabid/13489/Default.aspx. Last Accessed on April 26, 2022.

23Wilson, Benjamin, Data Privacy in India: The Information Technology Act (June 1, 2010). Available at SSRN: https://ssrn.com/abstract=3323479 Last Accessed on April 26, 2022.

24Salim, N. Breach of Privacy and Confidentiality under Information Technology Act, 2000. Legal Service India. https://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html Accessed on May 2, 2022.

25Supra Note 103.

[26]*Justice K. S. Puttaswamy (Retd) vs Union Of India.* Supreme Court of India W.P. (Civil) No. 494 of 2012 . 24 Aug. 2017.

[27]"Draft Personal Data Protection Bill, 2018." *PRSIndia*, 28 Jan. 2020, www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018. (Last visited on 22 April, 2022)

[28]"The Personal Data Protection Bill, 2019." *PRSIndia*, 24 Mar. 2020, www.prsindia.org/billtrack/personal-data-protection-bill-2019. (Last visited on 22 April, 2022)

[29]Dr Paranjape, N V. Studies In Jurisprudence And Legal Theory. 8th ed. Allahabad: Central Law Agency, 2016.

[30]Supra Note 108.

[31]Aggarwal , Naman M., et al. "India's Data Protection Bill." *Accessnow*, 24 Feb. 2019, www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf. (Last visited on 22 April, 2022)

[32]"Privacy Policy – Privacy & Terms." Google, Google, 31 Mar. 2020, policies.google.com/privacy. (Last visited on 22 April, 2022)

[33]"Privacy Policy – Privacy & Terms." Google, Google, 31 Mar. 2020, policies.google.com/terms. (Last visited on 22 April , 2022)

[34]Aggarwal , Naman M., et al. "India's Data Protection Bill." *Accessnow*, 24 Feb. 2019, www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf. (Last visited on 22 April, 2022)

[35]"Why Protonmail Is in Switzerland? An Analysis of Swiss Privacy Laws." *ProtonMail Blog*, 25 Mar. 2020, protonmail.com/blog/switzerland/. (Last visited on 22 April, 2022)

[36]M, Irina. "ProtonMail's Open Source Encryption Library Security Audit." *ProtonMail Blog*, 28 Nov. 2019, protonmail.com/blog/openpgpjs-protonmail-security-audit/. (Last visited on 22 April, 2022)

[37]Aggarwal , Naman M., et al. "India's Data Protection Bill." *Accessnow*, 24 Feb. 2019, www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf. (Last visited on 22 April, 2022)

[38]"Who, What & Why." *Have I Been Pwned*, haveibeenpwned.com/About. (Last visited on 22 April, 2022)

[39]Granville, Kevin. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens." *The New York Times*, The New York Times, 19 Mar. 2018, www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html. (Last visited on 22 April, 2022)

[40]Mihalcik, Carrie. “Marriott Discloses New Data Breach Impacting 5.2 Million Guests.” *CNET*, CNET, 31 Mar. 2020, www.cnet.com/news/marriott-discloses-new-data-breach-impacting-5-point-2-million-guests/. (Last visited on 2 May, 2022)

[41]Aggarwal , Naman M., et al. “India’s Data Protection Bill.” *Accessnow*, 24 Feb. 2019, www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf. (Last visited on 22 April, 2022)

[42]Aggarwal , Naman M., et al. “India’s Data Protection Bill.” Accessnow, 24 Feb. 2019, www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf. (Last visited on 22 April, 2022)

[43]Aggarwal , Naman M., et al. “India’s Data Protection Bill.” Accessnow, 24 Feb. 2019, www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf. (Last visited on 22 Nov, 2020)

[44]Delaney, Brigid. “Orwell's Nightmare Vision of 1984 Is Always Right Here, Right Now.” The Guardian, Guardian News and Media, 22 Oct. 2015, www.theguardian.com/stage/2015/oct/23/orwells-nightmare-vision-of-1984-is-always-right-here-right-now. (Last visited on 22 April, 2022)

[45]“Privacy Matters.” *Privacy Matters | Privacy International*, www.privacyinternational.org/learning-resources/privacy-matters. (Last visited on 22 Nov, 2020)

[46]Snowden, Edward, and Shane Smith. “'State of Surveillance' with Edward Snowden and Shane Smith.” *YouTube*, Vice News, 8 June 2018, www.youtube.com/watch?v=ucRWyGKBVzo. VICE on HBO: Season 4, Episode 13 (Last visited on 22 April, 2022)

[47]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 Last Accessed on 6 May 2022.

[48]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 Last Accessed on 6 May 2022.

[49]DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. (2000). Official Journal of the European Communities. https://doi.org/10.1039/ap9842100196 Last Accessed on 5 May 2022.

[50]Section 79, “The Information Technology Act, 2000”, Government of India.

[51]Madiega Tambiama, “Reform of the EU liability regime for online intermediaries”, EPRS | European Parliamentary Research Service (May 2020). Last Accessed on 5 May 2022.

52Bertolini Andrea and et al,“Liability of online platforms”, Panel for the Future of Science and Technology. EPRS | European Parliamentary Research Service. (February 2021). Last Accessed on 5 May 2022.

53Bertolini Andrea and et al,“Liability of online platforms”, Panel for the Future of Science and Technology. EPRS | European Parliamentary Research Service. (February 2021). Last Accessed on 5 May 2022.

54Agricultural Market Committee vs Shalimar Chemical Works Ltd, 1997 Supp(1) SCR 164, May 7, 1997.

55State of Karnataka v Ganesh Kamath, 1983 SCR (2) 665, March 31, 1983.

56Kerala State Electricity Board vs Indian Aluminium Company, 1976 SCR (1) 552, September 1, 1975.

57The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 Last Accessed on April 26, 2022.

58Article 19, The Constitution of India.

59Section 67, 67A, and 67B, The Information Technology Act, 2000.

60Shreya Singhal vs Union of India, Writ Petition (Criminal) No. 167 Of 2012, Supreme Court of India, March 24, 2015.

61The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 under the Information Technology Act, 2000. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf Last Accessed on 5 May 2022

62The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021? Last Accessed on 6 May 2022.

63Supra Note 141.

64WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA, Ministry of Electronics and Information Technology, Government of India. Last Accessed on

April 26, 2022.

65Article 5, General Data Protection Regulation of European Union.

66Justice K.S.Puttswamy (Retd) vs Union of India, W.P.(Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.

67Facebook Inc vs Antony Clement Rubin, Diary No 32478/2019, Admitted on January 30, 2020, Supreme Court of India.

68THE CHALLENGE OF MANAGING DIGITAL CONTENT, ITU-TRAI Regulatory Roundtable, 22 August 2017. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/August-RR-ITP-2017/ITU%20Report%20Regulatng%20Digital%20Content%202017%20Final.pdfLast Accessed on 5 May 2022.

69The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 under the Information Technology Act, 2000. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf Last Accessed on 5 May 2022

70The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 Last Accessed on 6 May 2022.

71The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 Last Accessed on 6 May 2022.

72The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PRS Legislative Research. (2022, May 5). Retrieved May 5, 2022, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 Last Accessed on 6 May 2022.

Revision #1
Created 6 November 2022 13:01:38 by ponytail
Updated 6 November 2022 13:11:23 by ponytail