
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

PROTECTION OF CONSUMERS' DATA AND PRIVACY – THE MOST PERTINENT CONSUMER PROTECTION NEED IN INDIA

- Roshni Rajani, Suyash Sisodia & Raghavendra Pai¹

ABSTRACT

Consumer Protection Act, 1986² ensures **Consumer Protection** in India. **Consumer Protection (Amendment) Act 2019**³ amended the legislation to remain in consonance with the advent of the **Internet** and act as a consumer protection law in India **post-liberalisation**⁴. The Act covers areas such as **product liability** and **false and misleading advertisements** while also subtly hinting at **consumer privacy**, which is the subject of this paper.

The Right to Life under **Article 21**⁵ takes the right to privacy. **Fundamental Right** which entails that no person shall have their information made known to anyone without consent. However, this gets **cloudier** when we talk about the **Internet** and **e-contracts** with long terms and conditions that can hide privacy clauses. **Data generation** has been the most extensive output of the internet era and even private browser or the incognito mode does **little to nothing** to keep your information private⁶.

Here lies the connection between **Data Protection** and **Consumer Privacy**. In a world where our privacy is accessible to corporations in the form of **Metadata**, data protection acts as a **person's privacy protection** due to the **integration** that our lives have had with the Internet. This paper attempts to look at **existing** laws that guide data protection in India and consumer's privacy protection and attempt to find **grey areas** to fill with **certain suggestions**.

Key Words: Right to privacy, Data protection, Consumer Privacy.

METHODOLOGY

¹ Students at Symbiosis Law School, Pune

² Consumer Protection Act, 1986.

³ Consumer Protection (Amendment) Act, 2019.

⁴ Burman, A. (2020). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? (pp. [i]-[ii], Rep.). Carnegie Endowment for International Peace. Retrieved July 9, 2021, from <http://www.jstor.org/stable/resrep24293.1>.

⁵ The Constitution of India, 1949, Article 21.

⁶ David Nielo, 'Incognito Mode May Not Work the Way You Think It Does', Wired (08-02-2020), Accessed on July 9 from <https://www.wired.com/story/incognito-mode-explainer/>.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

The authors of the poster have utilised doctrinal research as a methodology for conducting their research into consumer privacy and data protection in India with reference to the IT Act, Consumer Protection Act 2019 and the Data Protection Bill. It allows us to look at the existing legislation in India regarding the problems we face and make suggestions for the grey areas that exist.

Findings of preliminary research into the issue of Consumer Privacy in India

Consumer Privacy in India is maintained in the status quo under four measures -

1. In a **direct organisation-individual** contract, organisations might include privacy policies to ensure that it becomes the contractual obligation of the organisation to safeguard the individual's privacy
2. Via **General codes of conduct** that exist in professions such as medicine and other health service providers. These set rigid privacy norms for those working in that particular profession
3. Consumer Privacy disputes under the Consumer Protection Act have a **NATIONAL CONSUMER DISPUTES REDRESSAL COMMISSION**, set up under the Consumer Protection Act 1986, Section 21⁷
4. The **IT act** also imposes an indemnity against those that collect and control data in case of leakage or improper use of that data.

More profound research into the need for Consumer Privacy in India provide us with a few more findings -

- **560 Million** Indians have access to the Internet as of July 2020
- **1.1 Billion Mobile Data Subscriptions** as of February 2021
- Phone numbers, addresses, and E-mail IDs of all individuals that the government collects are **openly available** and often misused by service providers.
- No strong legislation holds those that breach privacy of consumer's data responsible for their **negligence or breach**

⁷Consumer Protection Act 1986, s 21.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

- The regulatory approach adopted in the Personal Data Protection Bill focuses mainly on protecting the consumers from their data being used in a manner that could be harmful to them. However, the bill doesn't specify those harmful practices.
 - **Sri Krishna Committee** said, *"A preponderance of evidence points to the fact that the operation of notice and consent on the Internet today is broken. Consent forms are complex and often boilerplate... Any enumeration of a consent framework must be based on this salient realisation: on the Internet today, consent does not work."*
 - In the modern rise of **Blockchain technologies**, information storage isn't centralised and thus becomes harder to regulate and protect. Due to no legislation that even acknowledges blockchain or bitcoin, all further legislations need to be created from scratch.
 - There is projected to be a **significant increase in compliance costs** if any data protection laws are implemented. It also asks for the creation of a separate commission to oversee data protection and consumer privacy in India.
 - The UK pays over **220 Million Pounds per year** and is expected to cost up to **2.1 Billion Pounds** in the first 14 years.
-

Issues that the paper attempts to tackle

1. How has the concept of **Consumer Privacy** and **Data Protection** evolved in India and other jurisdictions globally?
 2. What form of **legislation**, if any, already exists in **India** pertaining to Data Protection and Consumer Privacy?
 3. What are the **shortcomings** of these **legislations**, and what can be done to fill their gaps?
-

Cases that Formed the current state of Consumer Privacy and Data Protection Law

Two sets of landmark cases have led to our current understanding of Consumer Privacy and Data Protection. These are essentially National and International, the former important due to it being the law of the land and also as a mechanism to highlight our core argument that the natural state of progression demands further legislation in certain aspects while the latter, due to the common law nature of our judicial system that allows the ratio of various judgments to be utilised as reasoning despite it being in different countries. It is also done due to the nature of the cause of most data privacy problems being universal – the Internet.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

Indian Landmark cases and what they gave us -

- **Feldman vs Google**⁸ concluded that the click-wrap agreement was enforceable as there was a reasonable notice of the agreement along with mutual assent of the parties to it. Further, in **Hotmail Corporation v. Van Money Pie**⁹, it was held that clicking the 'I agree' button was sufficient to conclude a contract.
- In the Supreme Court's decision in **J.Samuel and others vs Gattu Mahesh and others**¹⁰, "due diligence is a requirement that cannot be dispensed with, and it determines the scope of a party's constructive knowledge." The *due diligence* or the required steps to be undertaken by the corporate bodies to obtain protection under the same are that the intermediary must not deceive or mislead the addressee about the origin of such messages.
- The Supreme Court in **Saiyed Rashedakhatun Vs. Vishnubhai Ambalal Patel**¹¹ has held that "*Due diligence means reasonable diligence; it means such diligence as a prudent man would exercise in the conduct of his affairs.*"
- In **Chander Kanta Bansal V. Rajinder Singh Anand**¹², while stressing the need for due diligence, a landmark judgment of the Supreme Court was referred by the Delhi HC for understanding the application of due diligence to social media platforms and e-commerce websites.
- **Postmaster, Rajinder Nagar Post Office v/s Ashok Kriplani**¹³ was one of the first cases where consumer information and privacy were given importance. In this case, the respondent's right to privacy had been infringed by the particular postman who tore a registered letter and compensation for the same was provided to the respondent under relevant sections of the Indian Post Office Act.

⁸Feldman v. Google, Inc. 513 F. Supp. 2d 229 (ED Pa. 2007).

⁹Hotmail Corporation v. Van Money Pie [1998] WL 388389.

¹⁰J.Samuel and others vs Gattu Mahesh and others, [2012] 2 SCC 300.

¹¹Saiyed Rashedakhatun Vs. Vishnubhai Ambalal Patel [2014] (MANU/GJ/0645/2014).

¹²Chander Kanta Bansal V. Rajinder Singh Anand [2008] 5 SCC 117.

¹³Postmaster, Rajinder Nagar Post Office v/s Ashok Kriplani, [2010] CPJ310(Del.).

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

- In the recent case of **Rishi Dixit and Ors. Vs Preventive Life Care Pvt. Ltd¹⁴**, the Telecom Disputes and Appellate Tribunal of New Delhi emphasized the need to distinguish knowledge from data and held that Section 43 of the IT Act does not bar the use of domain knowledge but prohibits copy, download or extraction of data, database or information in an unauthorised manner. The tribunal also directed the appellant to pay compensation for unauthorised data theft to the respondent u/s 66. The same was also held in **Gagan Harsh Sharma and Ors. Vs The State of Maharashtra and Ors¹⁵**.
- In **Justice K S Puttaswamy Retd And Another v Union of India And Others¹⁶**, it was held that an individual has the right “*to exercise control over his data and to be able to control his/her existence on the internet.*” The unauthorized use of such information may lead to a violation of this right. However, it was also held that the right to privacy is not absolute, and any breach of privacy, either by state or non-state actors, must fulfill the triple test of Legitimate Aim, Proportionality and Legality.

International cases and their contribution -

- In **Stevenson v. Henderson¹⁷**, it was held that any person who delivers any document to a person should give the required notice about the terms and conditions of the contract or the agreement. Similarly, the data controller must ensure that the privacy policy is provided in an easily accessible manner on the platform.
- In the suit against Google for misuse of consumer information and breach of the Data Protection Act 1998 DPA for the collection of browser-generated information (BGI) and the secret blanket tracing and collation of information, the judgment of **Vidal-Hall v Google Inc (The Information Commissioner intervening)¹⁸**, classified the misuse of private information as a tort. It allowed claimants to recover damages under the Data Protection Act 1998 (DPA) for non-material loss.

¹⁴Rishi Dixit and Ors. Vs Preventive Life Care Pvt. Ltd (MANU/TD/0024/2019).

¹⁵Gagan Harsh Sharma and Ors. Vs The State of Maharashtra and Ors [2018] (MANU/MH/3012/2018).

¹⁶Justice K S Puttaswamy Retd And Another v Union of India And Others [2018] Air Online [2018] Sc 237.

¹⁷Stevenson v. Henderson [1873] SLR 11_98.

¹⁸Vidal-Hall v Google Inc (The Information Commissioner intervening), [2015] EWCA Civ 311.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

- In **Australian Information Commissioner v Facebook Inc (No 2)**¹⁹, the Commissioner claimed/sought a civil penalty for **each Act of disclosure of personal information** by Facebook to Global Sciences Research Ltd (GSR) rather than for a single breach. It increases the scope of maximum quantum of the penalty that can be imposed and also sets a higher threshold of responsibility for such Big Tech companies, which host sensitive personal data of millions of people.
 - In the case of **WhatsApp Inc. v. NSO Grp. Techs., Ltd.**²⁰, where the NSO Group used the spyware 'Pegasus' to hack the phone devices of 1,400 users across the countries in the world, the court did not get convinced by the argument that NSO had no intention of breaching the data of WhatsApp users. It gave the decision in favour of WhatsApp, allowing the suit to proceed.
-

Contemporary developments in the Jurisprudence

Similar to the bifurcation of landmark cases into two, the contemporary cases are split into national and international. While the purpose of understanding current law and the law of the land with regards to the current state of affairs is to grasp better the world we are living in, we utilise this to show that there has been a very explicit evolution in this particular field of law not just nationally, but globally. It highlights that the stakeholders are no longer small city-states or local bodies, let alone State governments and Nations. It happens to be every individual on the planet with access to the Internet that consumes the product and service provided for by large Multinational Corporations regardless of age, sex or religion.

The current state of affairs in India

- **Section 43A of the Information Technology Act, 2000**²¹, read along with the Information Technology Rules²², requires every business in India, which collects, receives, possesses, stores, transmits, processes or can associate pretty much any other verb with 'personal information directly under a contractual obligation with the provider of information, **to have a privacy policy.**

¹⁹Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307.

²⁰WhatsApp Inc. v. NSO Grp. Techs., Ltd., [2004] 472 F. Supp. 3d 649.

²¹Information Technology Act, 2000, s 43 (A).

²²Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Sensitive Information Rules").

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

- One of the **essentials for a privacy policy** is the manner of presentation of the privacy policy to the user. It should not be presented in a way that is merely perfunctory to be placed on the website without the user taking notice of it, but it should be brought to the clear notice of the user and written in a manner that is understandable to the user; this is a crucial requirement for his **consent**. Furthermore, the privacy policy must explicitly specify the type of personal and sensitive personal data or information that it collects, the purpose of collecting such data, third parties to which such data can be disclosed, and the reasonable security practices to be adopted in order to prevent a data breach.
- **Section 5 of the IT Act, 2000**²³ also mentions that before gathering confidential personal data or information, the body corporate or any person working on its behalf must obtain consent written permission from the supplier of such data or information regarding the intent of use and further mentions that the data is received for a lawful reason relevant to a role or operation
- The section further provides that the corporate body must ensure by taking necessary steps that the person whose data is being collected must be made aware of the details of the agency retaining and collecting the information and also provides that the information shall only be used for the purpose for which it was being collected in the first place.
- In its report to the planning commission, the centre for the internet and society has established a structure according to which **nine principles** must be complied with to maintain privacy and protect data-related breaches.²⁴
- **Consent** of the user is the most crucial aspect of a privacy policy. The Supreme Court has in the landmark **Puttaswamy judgment**²⁵ held that every individual must ask permission or consent, which helps in safeguarding their rights which applies to both physical form and technology.

²³Information Technology Act, 2000 s 5.

²⁴Justice AP Shah et al., 'Report of the group of experts on privacy', planning commission, government of India, 2012, <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf>.

²⁵*Supra* Note 10.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

- The Income Tax Appellate Tribunal explained in the **enforceability of click-wrap contracts**, where the online user clicks on “I agree”, that though the requirements of a valid contract may be fulfilled, click-wrap contracts case the contract should not lead to contravention with the law of the land or contract is an electronic bargain. The tribunal explained where the contract terms are numerous, and in great detail, users often do not read through the terms, but that does not affect the validity of such contracts.
- As per **Section 79 of the Information Technology Act, 2000**²⁶, “*the intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of the transmission, and select or modify the information contained in the transmission*”.
- As per **Section 43 of the IT Act, 2000**²⁷, if any person, who is not the computer system or computer network (as defined in Section 2 of the said Act), without the permission of the owner or any other person who is in charge of such computer, computer system or computer network- causes breach of consumer data in contravention of the provisions of this Act, rules or regulations made there under, shall be liable to pay damages by way of compensation to the person so affected under **Section 66 of the IT Act**.²⁸

Recent International Developments

While there have been a plethora of recent developments internationally, these few events are key takeaways. They have been mentioned to act as a mechanism by which we add similar aspects to a prospective holistic law in India. Few recent developments include –

<p>Rights of Data Principal pertaining to Data Processing.</p>	<p>Role of Data Fiduciary (the entity that collects or processes a data principal’s data) and Data Processor.</p>	<p>Classification of Data: Personal Data; Sensitive Personal Data; and Critical personal data</p>
<p>Right to Data Portability: The right to receive the data from the fiduciary in a machine-readable format.</p>	<p>The right to be forgotten: The right to restrict continuing disclosure of personal data.</p>	<p>The GDPR allows data processing for prevention, investigation, detection, or prosecution of criminal offences and also discusses “public security”, “defence”, and “judicial” proceedings.</p>

²⁶Information Technology Act, 2000
²⁸Information Technology Act, 2000
 For general queries or to s

As per the **GDPR**, data processing should be allowed when the individual allows/consents for it. Consent carries similar meanings, with words like “free”, “specific”, and “informed”.

What more do we need?

We have noticed with the strong hard look that we have had at legislation and judgements that have commented on or given rise to newer questions with regards to Consumer Privacy and Data Protection that there exists a very urgent and pertinent need for new legislation that would encompass all the holes left in the system of providing protection to a consumer's privacy. The question is, what exactly are these things that are lacking?

1. Data Protection Bill tabled in parliament is not detailed in the sense that most activities that are to be charged with a penalty are not defined clearly (Harmful usage of data).
2. The Data Protection bill does not have any angle that provides us with a perspective into the rising Blockchain sector
3. Blockchain is essentially the decentralisation of data with an attempt at mutual checks and balances. It is also the platform that gave rise to Bitcoin.
4. Agreements used online in most cases are browse-wrap agreements that do not act as an active acceptance, making the consent dubious at best.
5. Multinational companies with all the data have almost no government regulation, and they are governed by laws that they self-impose. It calls into question both the authority of the government and the validity of self-imposition when the point of contention deals with sensitive personal information

Once these issues have been articulated, we may conclude the solutions that can be provided to them. However, before we take a look at it, it is pertinent to note why such changes are needed in the first place. Let us take you back to one of the earlier cases of **Postmaster Rajinder Nagar Post Office v/s Ashok Kriplani**.²⁹In this case, the Act of opening a person's post without their consent is wrong. All the complicated arguments boil down to this essential principle that it is wrong to view someone's information without their permission regardless of the degree of sensitivity. It is mainly to ensure that we value every individual's personal space and freedom while also setting a standard for the rest of the world. So how do we propose to do the same? What are our **Solutions**?

Not what we want but what we need

²⁹*Supra* Note 7

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

The solutions that we are going to provide might have two significant rebuttals to them -

1. The cost of compliance and the expenses incurred by the companies would make them less likely to invest in India
2. It would take a substantial legal workforce to exercise and implement and thus cost a lot to the government.

We would suggest here that the suggestions we provide are not meant to be a nuanced mechanism that would benefit all parties involved but rather a firm set of essential standards in the ambiguous state of affairs we currently reside in; this means we hold the protection of a person's privacy to the same standards as we hold the protection of our environment and want this to be the bare minimum that is followed in our nation. Moreover, these suggestions are not what we want, but what we need due to their integral nature.

Our suggestions are two-fold. These are suggestions made to both the government and the corporations that hold personal data.

Suggestions as policy proposals

1. Legislation – There are two forms of legislation required, one the very essential Data Protection Bill, and another a much more nuanced version that includes an understanding of the Blockchain environment. However, the Data Protection Bill rejected by the parliament had flaring issues, and a committee must look into the problems in order to propose a much more relevant legislation
2. Upholding only Click-Wrap Contracts so as to set a norm that would make free consent essential to all online agreements that deal with any data transfer. It would solve the issue in relation to many Browse Wrap agreements.
3. Having a Higher onus on Big Tech because they host personal/sensitive data of millions of people, and there exists no form of regulation on MNCs. Moreover, we would suggest a robust international framework for the same due to the fact that most of these MNCs store their consumer's data outside the jurisdiction of the consumer's country.

Critical Suggestions

1. The intermediaries and websites must **review their practices** and the practices of third parties that have access to the customer's personal information and ensure that they are not detrimental to the customer. They should also ensure that all their policies, terms and conditions, and other legal requirements are duly complied with.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

2. Such companies must consider providing **opt-out features** to the users if they wish to erase their information wholly or partially from the public domain or their website. It will make the companies dealing with consumer data more flexible and grant the people their right to be forgotten.
 3. Another step that such companies can take is to make the users aware of their policies, terms and conditions in lengthy documents written in legal parlance and provide short, **easy-to-understand summaries** of such terms and conditions. They should ensure that all the essential clauses are highlighted so that it is absolutely clear for the user to read and understand without fail.
 4. With regard to the **disclosure of consumer information**, the company must make the consumer aware of all the ways in which their data can be used and **take consent** for all such disclosures in the terms and conditions themselves. However, the company should also **ensure that such disclosure is not arbitrary**, against the consumer's interest, against public policy, or something that might otherwise cause inconvenience to the consumer. Further, sufficient steps must be taken to ensure the **security and safety** of such information.
 5. Such companies that indulge in disclosing consumer data to third parties must retain comprehensive records of the personal information disclosed to third parties and keep it updated regularly. This way, consumers' data will be safer and more secure in the hands of the companies.
-

To a safer and secure Future

The paper's main objective was to **highlight** the issues we face in **today's environment** with regards to Data Protection and Consumer Privacy and then take it a step further to suggest **solutions to implement**. However, this also acts as a document that gives you a **brief history** of Consumer Privacy Law in India and across the world. It is essential for the same to be noted because we have noticed from the beginning of consumer law that the idea was to side with the consumer. **'Customer is always right.'** is a term that goes ahead and highlights the importance that a **consumer** has.

So, on the same lines, the paper has **attempted** to bring back the **rights of consumers** into their own hands by forcing **large corporations** to **comply** with a much more **nuanced consenting**

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

methodology. At the end of the day, all because this is a toast we make in hopes of a different future where we do not have to worry about our **information** permanently being etched into platforms **without** our **consent**. ‘To a safer and much more secure future.’

Bibliography

Statutes

- Consumer Protection Act, 1986.
- Consumer Protection (Amendment) Act, 2019.
- Information Technology Act, 2000.
- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Sensitive Information Rules").
- The Constitution of India, 1949

Cases

- Feldman v. Google, Inc. 513 F. Supp. 2d 229 (ED Pa. 2007).
- Hotmail Corporation v. Van Money Pie [1998] WL 388389.
- J.Samuel and others vs Gattu Mahesh and others, [2012] 2 SCC 300.
- Saiyed Rashedakhatun Vs. Vishnubhai Ambalal Patel [2014] (MANU/GJ/0645/2014).
- Chander Kanta Bansal V. Rajinder Singh Anand [2008] 5 SCC 117.
- Amway India Enterprises Pvt. Ltd. v 1MG Technologies Pvt. Ltd. [2019] (260 MANU/DE/2146/2019).
- Postmaster, Rajinder Nagar Post Office v/s Ashok Kriplani, [2010] CPJ310(Del.).
- Rishi Dixit and Ors. Vs Preventive Life Care Pvt. Ltd (MANU/TD/0024/2019).
- Gagan Harsh Sharma and Ors. Vs The State of Maharashtra and Ors [2018] (MANU/MH/3012/2018).
- Justice K S Puttaswamy Retd And Another v Union of India And Others [2018] Air Online [2018] Sc 237.
- Stevenson v. Henderson [1873] SLR 11_98.
- Vidal-Hall v Google Inc (The Information Commissioner intervening), [2015] EWCA Civ 311.
- Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

- WhatsApp Inc. v. NSO Grp. Techs., Ltd., [2004] 472 F. Supp. 3d 649.

Journals and Articles

- Justice AP Shah et al., 'Report of the group of experts on privacy', planning commission, government of India, 2012 , <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf>).
 - Burman, A. (2020). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? (pp. [i]-[ii], Rep.). Carnegie Endowment for International Peace. Retrieved July 9, 2021, from <http://www.jstor.org/stable/resrep24293.1>.
 - David Nielo, 'Incognito Mode May Not Work the Way You Think It Does', Wired (08-02-2020), Accessed on July 9 from <https://www.wired.com/story/incognito-mode-explainer/>.
-

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>