



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

BLIND ACCESS TO PERSONAL AUTONOMY

BY PRIYANKA KHAWALE

ABSTRACT

The greatest lie on the internet is the one any user repeats daily by clicking “I have read and agree” without actually reading a single page. Privacy Policy, an important legal document that ensures transparency between the companies and internet users yet it rarely achieves that purpose. Users often tend to accept the privacy policy without reading them, as access to the service depends on acceptance. This raises a question whether such consent obtained is legally meaningful?

WHAT IS A PRIVACY POLICY?

Privacy policy is a vital legal document that explains the details of how the personal data of users is collected, used, stored and protected. It emphasizes the purpose for collection, third-party sharing and users rights on their obtained data.

It is also designed to shield companies from lawsuits as every time one downloads an app or opens a website the mandatory pop-up contents are usually the privacy policy or terms and conditions which explains about the site or app and the data they will have access to once the user clicks ‘I agree’. Since one has to give the consent manually, it acts a leverage for the companies as it is presumed that every user accepts or clicks the button only after reading the whole terms mentioned; however, ironically this isn't the scenario.

UNREAD AND UNTOUCHED

The question here is why do users simply overlook a document of such importance? People skip reading the privacy policy for several interconnected reasons such as:

1. Length and time:

The very first reason any person would state is that privacy policies are too *lengthy* to read and *time consuming*. No user wishes to spend almost fifteen minutes just to figure

out how their data is dealt with and who bears the responsibility if the personal data is misused. When the choice is between spending fifteen minutes to read a heavily drafted legal document and availing the service user needs, policy always loses.

2. Legal jargon:

Any user who sits down with a commitment to read the privacy policy, often gives up by the second paragraph as companies frame their privacy policies with complex legal terminologies which makes it difficult for a layman to understand the clauses mentioned. Policies drafted which are meant to emphasize on users data often boldly recognize the companies liability. Such kind of privacy policies are written with the notion to not make them clear and readable, but to make them legally bulletproof.

3. Language Barrier:

Especially in India another issue arises with the *language barrier*, most of the privacy policies are available only in English. This limits the vast majority of the regional language population from understanding even the basics highlighted in the policy. Although the [Digital Personal Data Protection Act, 2023](#) addresses this by allowing the notice to be not only in English but also in other regional languages, yet the implementation of the same by the companies remains a query untouched.

4. Take it or Leave it acceptance:

Privacy policies can be termed as non-negotiable standard form contracts. Users often tend to skip the reading because they are well aware of the lack of option to modify a clause they disagree with in the privacy policy. And refusal to such, because of a single unacceptable or uncomfortable clause, would cost them to lose the service. This reflects the imbalance of bargaining power between the companies or service providers and users, who can only accept them. Legally such contracts are recognized as contracts of adhesion, where consent is formally given but not freely negotiated.

5. Lack of Alternative:

Such imbalance of bargaining power gets worse when users have nowhere else to go beyond because many platforms have no substitutes. For instance, Riya wishes to open an Instagram account after noticing that all her friends are already having one. Being a keen person, she reads all the legal documents to understand how the app handles personal data, she comes across a pretty minor yet uncomfortable clause. In this scenario, Riya can either choose to opt out and not create an account or she can bear the discomfort and just accept and create an account. Taking Instagram practically does not have an alternative competing platform to substitute, it's likely that Riya would choose option two. The above scenario emphasizes the network effect, a service's value comes from the people already on it, so users stay even when they disagree with its terms. Especially when alternatives are weak or unavailable, accepting the policy becomes a necessity rather than a choice.

6. Conditioned Reflex:

Users have developed a naturally learned automatic conditioned reflex of clicking “accept” on every pop up that appears on every app and website without actually analyzing. This conditioned reflex is also a consent fatigue to the repeated action making users free consent look doubtful.

7. Lack of Digital Awareness:

Amongst the population accessing the internet, many users do not realize the purpose of collection of their data by the companies. In the initial years of the internet, it was reasonably presumed that corporations had little interest in any user's personal information. But today, personal data is equivalent to the digital economy. For instance, you search for a pair of shoes on any shopping site, later within hours, similar shoes advertisements appear on your social media app. It may feel like a coincidence or even surveillance to an extent but these are merely impacts of accepting privacy policies without reading them. Digital awareness enables users to understand the importance of reading certain legal documents in order to ensure safety of their own personal data and companies' liabilities towards that data.

REASONS TO CARE

It is often believed, privacy policy draws attention to the detail of knowing who is receiving your data but there are many other reasons which are beneficially for the user because apart from knowing who you are giving your data to, one might also find some interesting tools in these policies that'll give you more control over your own information. Several such reasons make it worth reading.

1. Data receiver: Policies disclose in detail who holds and shares your data apart from the company, app or website. It encloses the details of whether the data is shared with third-party services or any advertisers. It is the answer to the most asked query “who am I giving it to?”
2. Prevention from cyber crimes: Recent statistics of cyber crime actively portray a bigger picture of how the data is dealt. The [National Cyber Crime Data](#) records hike in the cyber crime report for the year 2024. The Annexure II of the report addresses various cyber offences commonly committed include breaches of confidentiality and privacy, data theft, financial fraud and cyber blackmailing, all of which depend on the access to personal data. Understanding the basis of collection and preventive measures any platform provides helps users secure their personal and financial data, while analyzing the risk before they hand over their data. Here, reading the privacy policy can be interpreted as a form of self-protection.

3. Statutory Rights of Data Principal: [Section 11 of the Digital Personal Data Protection Act, 2023](#) provides data principals the right to obtain summary of their provided personal data. While [Section 6\(4\) of the Digital Personal Data Protection Act, 2023](#) provides data principals the right to withdraw their consent at any time. And under [Section 12\(1\) of the Digital Personal Data Protection Act, 2023](#) states right of the data principal to correction, completion, updating and erasure of the personal data. These provisions work as an accountability mechanism on the companies, apps or websites holding them liable to the users and safeguarding the data. These provisions exercised through privacy policies remain undiscovered by the users who ignore the policy.
4. Lifecycle of Data: Policies mention the time period of how long one's personal data would be stored and what happens after the user leaves.

Consider Andrew used a food delivery app just once to order. He agreed on every pop up of documents without actually reading them. Later, he deleted the app. Even after deletion of the app would his data still be stored? Yes, every personal data input by him to place even that single order may remain stored until he deletes the account rather than the app. We usually notice every time we re-download any app it seems to recognize your device often because the reason behind it are the clauses mentioned in the privacy policy.

5. Personal autonomy: Time and again, users' feeds are influenced through the analysis of the data collected. The advertisement and recommendations influence what users see, buy and believe. This helps users with informed choices and autonomy.
6. Parental consent: Beyond general users, an aspect of digital safety of minors cannot go unaddressed. The [Digital Personal Data Protection Act, 2023](#) mandates parental consent for processing child data to safeguard children and adolescents from unintentionally providing access to their data to fraudsters. The vulnerable age groups are likely to be targets of misuse hence regulation of verifiable parental consent while accepting policies safeguards children's data.
7. Standard form contracts: The greatest presumption regarding privacy policy is clicking 'I agree' doesn't make much of a difference. But little does one understand, clicking 'I agree' leads to creation of a contract between the users and the companies. Since privacy policies include terms on arbitration, limits on liability or even cross-border transfer of data, the user is bound by the obligations irrespective of whether they read it or not.
8. Choices: Concisely, a user who reads companies policies would choose a better platform for service, while safeguarding his personal data.

FREE CONSENT AND LEGALITY

The concept of consent needs to be understood with the unambiguous definition defined under [Section 13 of the Indian Contract Act, 1872](#). It clearly states that the parties to the contract are said to consent when they agree on the same thing in the same manner. Consent works on the principle of *Consensus ad idem* which translates to meeting of mind. [Section 14 of the Indian Contract Act, 1872](#) establishes when the consent is said to be free when it is not influenced by external factors such as coercion, undue influence, fraud, misrepresentation and mistake.

Free consent is plausibly a myth when privacy policy is materialized. As established earlier, privacy policy leaves not much of a choice to the users not clicking ‘I agree’ involves a trade off of services. The bargaining power absolutely lies in the hands of the policy maker and very less to the user. The ‘take it or leave it’ privacy policy contracts become a choice only at the option of presence of alternative platforms with better policies. User rather than waiver accepts to proceed.

[General Data Protection Regulation of the European Union](#) lays a foundational step for the Indian legislation of the [Digital Personal Data Protection Act, 2023](#). [Article 4\(11\) of the GDPR](#) regulates valid consent and [Article 7 of the GDPR](#) requirements for valid consent. These four requirements are expressly addressed with an addition under [Section 6 of the Digital Personal Data Protection Act, 2023](#) mandates valid consent to be free, specific, informed, unconditional and unambiguous. It also requires the consent to be withdrawable so that users have the control over their personal data. It provides a better mechanism to protect the users when privacy policies limit liabilities to protect the companies.

Although valid consent defined under [Section 6 of the DPDP Act, 2023](#) requires it to be unconditional, the query remains the same. Can the consent be unconditional if refusing means losing the service? Unlike the [Digital Personal Data Protection Act, 2023](#), [GDPR](#) forbids bundling consent under [Article 7\(4\) of the GDPR](#). The rule against bundling consent refers to the act of forcing a user to accept extra data processing for a non-negotiable condition or signing a contract. This provision narrows the scope of acceptance of privacy policy and gives choices to users. And the privacy policy no longer remains a ‘take it or leave it’ contract.

[Meta Platforms Inc. and WhatsApp LLC vs. Competition Commission of India, 2025](#)

The Competition Commission of India (CCI) took a suo motu cognizance of the mandatory “take it or leave it” terms of 2021 WhatsApp's Privacy Policy. CCI ruled that WhatsApp had abused its dominant market position, forcing the users to agree to expanded data sharing with other Meta entities as a condition to use the app. CCI imposed a heavy penalty of Rs. 213.14

crore and issued a cease and desist directive including five years ban on sharing user data for advertising purposes.

However, Meta and WhatsApp appealed before the National Company Law Appellate Tribunal (NCLAT). The Tribunal upheld the penalty nevertheless removed the five year ban on data sharing. CCI cross- appealed in the Supreme Court while WhatsApp agreed to comply with the other NCLAT directives.

The landmark precedent laid under Meta Platforms Inc. and WhatsApp LLC vs. Competition Commission of India, 2025 emphasizes that no platform can force a take it or leave it agreement on the users.

BEHIND THE “CLICK”

The decision upheld by the National Company Law Appellate Tribunal shows that no platform can abuse its position, but this decision was taken after millions of users for years had already clicked “accept”. In other words, the remedy came after the damage was done. But to actually understand what users agree to and how the policy is structured, it is necessary to know what happens behind the click.

The journey of a click begins the moment the user accepts a privacy policy. As soon as ‘I accept’ is clicked, the platform collects various data of the user, which a user may manually insert or just allow through permissions. The data collected usually includes name, phone number, location, access to gallery, contacts and various other permissions. But the platform also collects the data which a user may be unaware of, this kind of data is generated by users' behavior, it includes searches, clicks, time spent on a particular site, likes and dislikes. The data generated through behavior is analyzed to build the user's profile and condition it according to users' interests and habits. It helps platforms to provide personalized content advertising, which helps them reach out to a specific kind of users.

To illustrate, Sana and her friends plan for a trip to Manali. They collectively start searching for suitable tours and travels, hotels and sightseeing places on web browsers. The moment she opens her social media app, she comes across a pop up of an influencer advertising a hotel of the same location they are planning to go. In this scenario, it is rarely a coincidence, rather, it is the consequence of clicking ‘I agree’ without reading the privacy policy. Many platforms usually include the consent to cross-site tracking and real-time data exchange between two or more independent platforms. These kinds of invisible handshakes are actually results of not only behavioral personalizations, but also targeted personalization. By failing to read the privacy policy, users are often unaware of their browsing habits being particularly scrutinized, transforming their feed into a targeted commercial ecosystem.

Underlying Sana's experience, let's understand how the invisible handshake works. Often websites, apps and platforms track users through small tools, like cookies and advertising ids. These tools record the user's searches and visits, allowing advertising agencies to pop up ads or other relatable contents to customize the user's feed. However, the question remains: do policies not address cross-site tracking? Privacy policies usually recognize these small tools as "Partners" or mention the term "as necessary", this allows companies to use data in many ways. Although the [Digital Personal Data Protection Act, 2023](#), mandates only necessary data collection, still, the app often requests for the access of conducts, location and gallery even when the service does not need it. It demonstrates transparency only exists on paper, and the users cannot easily find the answers that matter.

CONCLUSION

The phrase "I have read and agree" is no longer a statement of fact, but more like an involuntary ritual done by the users. Users skip reading privacy policy over simple reasons of it being lengthy, time consuming, written with various incomprehensible legalese and often available only in English, but the major reason, which remains unnoticed is the lack of digital awareness among the users. Due to the illusion of competence, many users assume that they know what is written in the privacy policy and hence they choose to bury their heads in sand. Either they find privacy policy irrelevant or simply self-explanatory due to the illusion. The perspective of users towards privacy policy can be understood through a very simple observation that reading would cost time and change nothing. So they instead choose a rational response to involuntarily accept them.

The [Digital Personal Data Protection Act, 2023](#) requires the consent to be free, specific, informed, unconditional and unambiguous by interpreting a clear rule against forcefully imposing user's consent to avail the service. The law recognizes the problem and formulates provisions to safeguard the users. The Judiciary interprets remedies against the act of "*take it or leave it*" terms addressing and predicting the problems of the future. But the fact to be borne in mind is that the remedies still rest on the assumption that the user's consent to click "I agree" is out of real choice and not a fictional consent.

This burden of presumption should be shifted to the policy drafters, rather than being placed on the users. Companies should genuinely collect only that part of the data that they need from users irrespective of whether the user reads the policy or not or companies should switch to a simply drafted privacy policy that would guarantee a much better effect for both the users and the companies. A privacy policy should either be a short summary with layers of understated legal enforcements, or should be available in regional languages for the population. The privacy policy should move from relying on the user's fictional consent to actually regulating the company's conduct. In the meantime, "I have read and agree" will always remain the greatest lie on the internet.

BIBLIOGRAPHY

1. [The Digital Personal Data Protection Act, 2023](#)
2. [The General Data Protection Regulation](#)
3. [The Indian Contract Act, 1872](#)
4. [Meta Platforms Inc. and WhatsApp LLC vs. Competition Commission of India, 2025](#)
5. [National Cyber Crime Data](#)