engineering proceedings

MDPI

Proceeding Paper

The Consent Illusion: A Computational Systems Framework for Privacy Governance in Platform-Based Digital Tracking †

Preeti Devarakonda *, Chandrika Valluri, Peddi Sarayu Reddy, Ashish Marri, Abhilash Gajula and Abhijith Reddy

School of Law, Mahindra University, Hyderabad 500043, Telangana, India;
sl22ulbb009@mahindrauniversity.edu.in (C.V.); sl22ulbb037@mahindrauniversity.edu.in (P.S.R.);
sl22ulbb007@mahindrauniversity.edu.in (A.M.); sl22ulba011@mahindrauniversity.edu.in (A.G.);
sl22ulbb001@mahindrauniversity.edu.in (A.R.)

* Correspondence: sl22ulbb032@mahindrauniversity.edu.in

† Presented at the 8th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Aizuwakamatsu City, Japan, 27–29 July 2026.

Abstract

The governance of online tracking increasingly relies on consent-based privacy mechanisms established under frameworks such as the General Data Protection Regulation (GDPR), the e-Privacy Directive, the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA), and India's Digital Personal Data Protection Act (DPDPA). However, the continued expansion of behavioral tracking demonstrates that formal consent mechanisms do not necessarily provide meaningful control over personal data in technologically complex digital environments. This paper examines the Consent Illusion as a system-level privacy governance problem arising from the interaction of tracking technologies, interface design, behavioral profiling, information asymmetry, and platform-based economic incentives. The study employs a comparative doctrinal and socio-legal methodology to analyze regulatory approaches alongside the technical evolution of cookies, third-party tracking, device fingerprinting, server-side tracking, real-time bidding, and behavioral profiling. The analysis demonstrates that technology-specific restrictions can be circumvented through functionally equivalent tracking technologies, while consent interfaces can be weakened by consent fatigue, dark patterns, and asymmetries in information and control. Building on these findings, the paper proposes a Rights-by-Default Privacy Governance Framework that combines fiduciary obligations, data minimization, technology-neutral purpose limitations, and structural protections that operate independently of individual consent. The framework does not eliminate consent; rather, it treats consent as one component of privacy governance within a broader technical, legal, and institutional architecture. The paper argues that effective digital privacy protection requires a shift from regulating individual consent events toward governing the systems, data flows, interfaces, and organizational practices through which behavioral tracking occurs.

Keywords: digital privacy; consent-based regulation; cookie governance; behavioral tracking; platform capitalism; dark patterns; information fiduciaries; data protection law; informational self-determination; rights-by-default; privacy governance

Check for updates

Academic Editors: Debopriyo Roy, George Fragulis and Peter Ilic

Published: 16 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

The modern Internet is built upon interconnected technological systems that enable communication, personalization, authentication, transactions, advertising, and large-scale

data processing. Within this infrastructure, HTTP cookies were originally developed to allow websites to maintain state across otherwise stateless HTTP interactions, including user preferences, authentication sessions, and shopping-cart information. Over time, however, cookies became important components of digital tracking architectures through which websites, advertising networks, analytics providers, data brokers, and platforms collect and correlate information about users across websites and devices. These technical processes enable the construction of increasingly detailed behavioral profiles that can subsequently be analyzed and monetized. This transformation has contributed to the development of what has been described as surveillance capitalism, in which behavioral information becomes an economically valuable resource [1].

The privacy implications of these systems have led jurisdictions to develop regulatory frameworks based substantially on notice, transparency, choice, and consent. In the European Union, the GDPR and e-Privacy Directive impose requirements concerning consent before certain forms of non-essential tracking are deployed. In the United States, the CCPA and CPRA provide consumers with transparency and rights concerning the collection, sale, and sharing of personal information. India's DPDPA establishes a consent-oriented framework built around obligations imposed on Data Fiduciaries. These approaches differ in their legal mechanisms, but they share an important assumption: that individuals can exercise meaningful control over the processing of their personal information through legally recognized choices.

However, the continued prevalence of behavioral tracking raises a fundamental question about whether this assumption remains technically and institutionally realistic. Users are frequently presented with complex consent interfaces containing extensive information and multiple choices, while platforms possess substantially greater technical knowledge about how data is collected, processed, combined, profiled, and monetized [2]. At the same time, the restriction of one tracking mechanism can encourage the adoption of another technically different but functionally similar mechanism, such as device fingerprinting or server-side tracking [3]. The result is a fundamental distinction between regulating a technology and governing the underlying data-processing function.

From a Computer Science perspective, this distinction is important because behavioral tracking is not a single technology. It is an ecosystem composed of multiple technical components, including browser storage mechanisms, third-party scripts, identifiers, device characteristics, server-side processing, advertising exchanges, analytics platforms, databases, and profiling algorithms. A regulatory rule targeting one component may therefore leave the broader information-processing function intact.

The central argument of this paper is that the limitations of consent cannot be understood solely as failures of legal enforcement or deficiencies in individual decision-making. They arise from the interaction between technical system architecture, interface design, information asymmetry, behavioral influence, and platform economic incentives. The validity of consent therefore depends not merely on whether a user technically clicked an acceptance mechanism, but on the technological and institutional conditions under which that decision was produced.

While privacy scholarship has extensively examined both the technical architecture of online tracking and the legal regulation of personal data, these areas have often developed along relatively separate analytical paths [2–5]. There remains comparatively limited attention to cookies and behavioral tracking as a common intersection of technical design, regulatory governance, and structural power. This paper addresses that intersection by examining whether consent can realistically function as the primary governance mechanism within technologically complex and economically asymmetric digital environments [2,6].

https://doi.org/10.3390/engproc2026143095

The paper consequently asks whether the continuing limitations of privacy protection result primarily from weak enforcement and technological adaptation, or whether they reveal a more fundamental limitation in the assumption that individual consent can independently govern complex digital data-processing systems.

To examine this question, the study conducts a comparative doctrinal analysis of the GDPR, e-Privacy Directive, CCPA/CPRA, and DPDPA, combined with a socio-legal analysis of information asymmetry, platform capitalism, behavioral economics, and information fiduciary theory [2,7,8]. It also considers the historical evolution of digital tracking technologies and the regulatory responses to them. The analysis ultimately proposes a shift toward a Rights-by-Default Privacy Governance Framework, in which minimum privacy protections operate independently of whether an individual has technically provided consent.

The proposed approach does not seek to eliminate consent. Instead, it recognizes that consent is most meaningful when users have genuine alternatives, understandable information, non-manipulative interfaces, and sufficient practical control over the consequences of their decisions. Where those conditions cannot reasonably be achieved, privacy protection should not depend entirely on the individual's ability to navigate complex technical and economic systems.

The paper therefore reframes digital privacy as a system-level governance problem. Rather than asking only whether a user consented to tracking, privacy governance should also examine what tracking technologies are used, how information flows through the system, how interfaces shape user decisions, what purposes are served by the processing, whether data minimization is observed, and what responsibilities are imposed on the organizations controlling the relevant infrastructure.

2. Research Methodology

The methodology used for this study is comparative doctrinal methodology, which is supported by a socio-legal analysis. The purpose of this analysis is to evaluate the use of consent-based governance as a regulatory measure for various digital tracking technologies. The doctrinal analysis portion examines the regulatory framework controlling cookies and behavioral tracking activities under the General Data Protection Regulation (GDPR), e-Privacy Directive, the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA) and the Digital Personal Data Protection Act (DPDPA) enacted in India in 2023. By comparing these four instruments, it is evident that they provide various forms of privacy governance based on whether the privacy governance requirements consist of an opt-in consent process (i.e., GDPR), a transparency model (i.e., e-Privacy Directive), a model that relies on an opt-out process (i.e., CCPA/CPRA) or a combination thereof (i.e., DPDPA) [9].

Primary legal materials analyzed include legislative provisions, regulatory guidance from the various data protection authorities, case law and enforcement activities taken by each jurisdiction's respective data protection authority. Special emphasis is placed upon case law issued by the Court of Justice of the European Union related to consent requirements, such as Planet49 GmbH v Bundesverband der Verbraucherzentralen (C-673/17) and IAB Europe v Gegevensbeschermingsautoriteit (C-604/22) [10,11]. A review of the enforcement measures employed by European data protection authorities also provides a comprehensive understanding of how consent elements are developed and enforced. This study employs a socio-legal analysis and an assessment of the law using the socio-legal framework, which assesses how the law works within the broader technological, economic, and social context [12]. The study is informed by three theoretical perspectives. The Information Fiduciary theory helps to assess whether digital platforms should be subject to the fiduciary duties of loyalty and care to users, due to significant disparities of asymmetry

in information and power [7,8,13]. The Economics of Privacy provides a framework to examine how boundedly rational users make decisions based on the power imbalance created by information asymmetries [2]. Finally, Responsive Regulation theory provides a framework to analyze how digital platforms have used technological substitution and regulatory displacement to respond to legal prohibitions [14].

This study used HeinOnline, Westlaw, SSRN, Scopus, and Google Scholar to conduct a review of all legal, economic, and interdisciplinary research between 2011 and 2026. By combining both the doctrinal and socio-legal approaches, this study evaluates whether or not consent-based regulation is legally valid and whether it is capable of offering protections to users' rights to informational privacy.

The research is not experimental in nature nor does it provide new empirical data, but instead is based on the analysis and evaluation of legal rules, judicial proceedings, regulatory practices, and secondary literature. In this regard, any mention of effectiveness or insufficiency of consent in this paper should be regarded as doctrinal and socio-legal findings rather than empirical causal statements. The study relies on empirical investigations into cookie consent dialogs, dark patterns, and online tracking as background information for legal research and to show the realities of regulatory theories. It is necessary to note that the purpose of the research is not to measure user behavior but to study whether the legal structure of consent is capable of ensuring informational privacy in light of the current technology and economics.

3. Technical Framework of Digital Tracking and Its Regulatory Importance

The legal significance of cookies is not due to their existence but rather due to the role they play as tools of behavior tracking. The purpose of developing cookies was to resolve the issue of statelessness with regard to communication over the HTTP protocol. Cookies allow websites to store information they need in order to provide functioning services such as user identification, language selection, and shopping-cart information. Initially, cookies posed very limited privacy issues.

The current regulatory discussion surrounding cookies evolved with the proliferation of third-party tracking technologies. Third-party cookies are placed on an individual's browser by another entity (typically an advertising network, measurement/analytics provider, or social network) and can track an individual on multiple web pages, allowing these parties to consolidate behavioral data in order to create a complete picture of an individual [3]. The development of programmatic advertising and Automated Real-Time Bidding solutions further exacerbated these concerns because they involve data-sharing across many different platforms between advertisers, intermediaries, and data brokers [15,16]. When it comes to advertising, there are a lot of questions regarding the use of personal information and whether or not you have consented to its use. The ad-tech ecosystem (the way in which advertisers target you based on your online behavior) has created a very complex environment in which it is very difficult to determine who has obtained and collected personal information and how it has been processed [17].

As privacy legislation evolves in so much of the world towards a model based on the premise that individuals can both comprehend and manage the processing of their own personal data [18], the increasing complexity of modern ad-tech ecosystems complicates the identification of who has collected an individual's personal data, how it is processed, and what uses it will ultimately be put to, making this a governance issue as much as a technological one.

Regulators have started to acknowledge these difficulties; increasingly, the courts in the Planet49 and IAB Europe cases have recognized judicially what was once simply a technical

issue, namely, that consent mechanisms and the technologies that underpin them cannot be treated as separate entities [10,11]. Consequently, privacy regulations are not limited to website owners but are also extended to cover the larger advertising ecosystem, including how consent is obtained in those ecosystems through technological means.

Additionally, as technology continues to advance, there have been limitations identified concerning technology-specific regulations. For instance, as restrictions on third-party cookies have begun to be put into effect, there has been an increase in the use of other tracking techniques (e.g., device fingerprinting, server-side tracking), which, while differing from traditional cookies technically, provide similarly profiled, identified and tracked information regarding users across digital environments [3]. A challenge we often face in the digital regulation realm is that when one tracking technology is restricted, entities will migrate to a functionally equivalent tracking technology instead.

Cookies provide another great example because this technology can help to frame other broad issues about consent, informational asymmetry, and any related regulatory efforts surrounding the same. Thus, while the cookies represent a very important technology in their own right, their use also illustrates some of the larger privacy governance issues we currently face.

4. Governance Framework for Consent: A Comparative Law Approach

Different countries have developed different approaches to regulating cookies and behavioral tracking, and the European Union, United States and India each have different methodologies for regulating these issues, but they each start with the assumption that individuals will be able to exercise control (consent) over the way their personal information is collected and processed.

4.1. European Union: Consent as a Condition of Law

The EU has developed an extremely robust legal framework around cookies and other types of behavioral tracking, which comprises the e-Privacy Directive as well as GDPR [9,19]. Regarding the storage of information on a user's device, according to Article 5(3) of the e-Privacy Directive, user consent must be obtained unless it is strictly necessary for providing the service requested. Furthermore, under GDPR, there are additional requirements placed on obtaining consent which must be satisfied before one can be compliant with the regulation: to have obtained free, specific and informed consent from individuals regarding how they will utilize the data collected and to have obtained clear and unambiguous consent [20,21]. These measures have also been judicially clarified by the courts. In the recent case Planet49 GmbH v Bundesverband der Verbraucherzentralen, the Court of Justice of the European Union stated that a pre-checked box does not satisfy the requirement of consent [10].

In IAB Europe v Gegevensbeschermingsautoriteit (C-604/22), the Court agreed that consent signals created by the Transparency and Consent Framework could be personal data and indicated that entities involved with administering the transparency and consent framework could be considered joint controllers of that data [11].

Similarly, European regulators have developed a rigorous enforcement mechanism, particularly the CNIL, for which they have provided support examples demonstrating how consent interfaces provide consumers with options that are real and symmetrical [17]. Therefore, the European model is the first attempt at converting a formal requirement of consent into a substantive privacy protection mechanism.

4.2. The American Regulation: The Model Is Based on Transparency and Choice of the User as It Relates to Privacy

Traditionally, regulations governing privacy in the United States are market-driven, resulting in an emphasis on transparency and choice for the consumer rather than requiring the use of prior consent for the processing of personal data. The majority of federal enforcement actions are based on Section 5 of the Federal Trade Commission Act prohibiting unfair or misleading commercial conduct. The CCPA and CPRA are laws that protect consumers' rights to privacy in the state of California by granting consumers various rights regarding the information collected about them. The consumer rights included in these laws give consumers access to their personal data, the ability to delete that data, and the option to opt out of selling and sharing their information. In comparison, CCPA and CPRA grant consumers the ability to exercise their rights post-factum rather than requiring consent from consumers at the time of collecting data. The intent of the EU's laws is to limit the manner in which data can be processed, whereas California permits the collection of data but offers consumers the opportunity to use the privacy rights outlined in the CCPA and CPRA after their information has been processed. This variation becomes important regarding how California's laws and the EU's laws address privacy as both consumer protection and accountability.

4.3. India's Digital Personal Data Protection Act, 2023 (DPDPA)

The DPDPA is a monumental advancement in privacy legislation in India, established by the Supreme Court's ruling in K.S. Puttaswamy v. Union of India that privacy was an inherent right [22,23].

The DPDPA is built on the principle of consent and sets out specific requirements for obtaining consent, such as: must be freely given, specific to the purpose for which it was obtained, must be informed, must be given unambiguously, must be communicated in a sufficient manner, and must allow for the revocation of consent [24–26]. In addition, requests for consent must be in understandable language [27]. One of the main differences in the legislation is defining who a Data Fiduciary is [28]. A Data Fiduciary refers to an entity that determines the purpose and means of processing data, and this designation acknowledges that a major power imbalance exists between individuals and organizations that process their personal data. In addition to the Data Fiduciary, the DPDPA also creates a structure known as a Consent Manager, which is intended to allow for providing, managing and withdrawing consent for the use of data across digital service providers.

4.4. Comparative Notes

Even though there are significant differences among the European, American and Indian frameworks, they share a fundamental assumption: that the principal way to protect privacy is through individual choice. The EU protects individual choice by implementing strict legal standards; the US relies on transparency and individual decision-making, while India combines both consent and a fiduciary-type approach with institutional innovation.

However, each of these systems is dealing with similar challenges. Digital ecosystems are becoming increasingly complex, and as such, it is unreasonable for individuals to be expected to make decisions concerning their data's use given that the types of data use are generally opaque and technologically complicated. The primary question that will be addressed in this article is whether the reason that current privacy regulation has not worked well is mainly due to a lack of enforcement, or if the real problem resides in how consent has been assumed to be an effective governance tool in the current digital economy on its own.

5. Platform Capitalism's Political Economy and the Structural Constraints on Consent

The flaws of cookie regulations cannot only be viewed from a statutory or compliance viewpoint. The long-term persistence of behavioral tracking, despite the increase in more sophisticated privacy laws, reflects broader structural characteristics of the current digital economy. The constraints of consent-based governance will need to demonstrate their limits, analyzed through the political economy of platform capitalism, where personal data becomes more than information, but rather a viable strategic economic resource.

5.1. Human Experience: Behavioral Data and Commodified

Digital platforms have made a great deal of money from behavioral data through the gathering and analysis of data generated by every online interaction (e.g., searching for a product on an e-commerce website, interacting with content on an e-commerce website). Collecting this type of information (referred to as 'typical market-based transactions') is basically just taking what a user does and turning it into something useful for someone to do with (which you can see in Exhibit 4) [29]. Because behavioral data is created through human behavior, unlike traditional economic resources, it allows companies to turn the everyday user experience into something valuable for business purposes through surveillance capitalism; an example would be from social media or e-commerce sites [1].

The surveillance capitalist theories being produced by the growing digital economy also have implications beyond simply being able to identify users based on behavior to monetize that behavior via traditional advertising models. Platforms have demonstrated the ability to extract what has been termed 'surplus behavior' from users, essentially the data that was produced during that user's activity and can then be put to use to both analytically and monetarily exploit users [1]. This behavioral surplus essentially forms the foundation of targeted advertisements, algorithm-based recommendations, and predictive analytics, as the user's identity ultimately creates not just the data that was used to create the above outcomes, but also allows companies to gain economic and social power due to their knowledge of that user's behavior [30].

The commercialization of behavioral information has significant consequences for privacy regulations. Existing consent frameworks suggest that individuals can independently negotiate with companies regarding the collection and use of their data, based on their own autonomy. Nevertheless, because behavioral data represents a crucial revenue stream for businesses, these companies are heavily motivated to collect as much data as possible, often without securing genuine consent from individuals. As a result, privacy concerns are closely linked to wider market dynamics rather than being dictated solely by personal decisions.

5.2. The Difference Between Individuals and Companies in Terms of Information and Control

The operation of the current scheme of consent-based regulation assumes an approximate balance of power between individuals and data processing entities. In reality, however, there is an extremely large imbalance of informational power between digital platforms that own and process data and the individuals from whom the data is collected [25].

This asymmetrical relationship is also about more than just having different amounts of information. The operators of online platforms design user interfaces to allow companies to collect users' consent before they collect data about the user, and determine the way in which the data will be collected and processed [31]. These platform operators also have access to the technical expertise necessary to implement the design and processing of user data that is not available to the average user. People are generally required to make

privacy-related choices without knowing what happens after they provide their data, who else gets to see it or use it, or how companies will use algorithms to interact with them.

From a socio-legal standpoint, these differences in power dynamics interfere with the normative foundation of consent. Consent has legitimacy if the individual has been able to make an informed and free choice, but when one party has control of both the information and conditions of the decision being made, the authenticity of that choice is brought into serious question. This is about the overall power imbalance in the digital markets rather than just a compliance issue.

5.3. Platform Governance and Behavioral Influence

Digital platforms not only collect behavioral data but also shape the environments in which their users make those decisions. They influence how their users behave through the design of their interfaces, their recommendation systems and the way in which they create and present content to users [32,33].

This is particularly relevant to cookie consent and governance. Often, cookie consent interface environments are designed to maximize user engagement and to minimize user resistance to the collection of their data. Behavioral design techniques through the use of visual prominence, default settings and strategic interface architecture can create situations where users accept tracking without giving sufficient thought to the ramifications of tracking their behavior. The consent process cannot simply be measured by looking at whether a user clicked "OK" to an acceptance button; the conditions under which consent was given, particularly those related to the social and legal conditions at the time, should be considered as well. If consent is given in a situation where behavioral manipulation is prevalent, there is an uneven power balance between parties and thus, consent will legitimize the extraction of data rather than protect the autonomy of the individual.

5.4. Implications for Privacy Governance

The political economy of platform capitalism indicates that there are fundamental sources of tension between contemporary privacy regulation and the digital economy; where privacy law is primarily based on individual consent, the digital economy is being created around incentivizing large amounts of data collection and behavioral profiling. While technological limitations may exist in terms of cookie regulations, the limitations of cookie regulations are also related to an incongruence between the assumptions underlying the regulation of consent and the realities of the digital economy. To determine whether other forms of governance can adequately protect the information privacy of individuals, we must understand where the incongruences between the two originate.

6. The Failing Model of Cookie Governance Based on Consent

Privacy regulation today is based on the idea that individuals have some control over the collection and processing of their own data by exercising their right of consent. Organizations across multiple jurisdictions use consent as the primary way to gain legal authority for conducting behaviorally-based tracking of individuals. However, as many scholars now contend, it seems very unlikely that individuals really have or can effectively exercise meaningful control over their personal data as a result of the limitations of existing cookie governance. The issues associated with cookie-based governance are not simply aggravating occurrences of non-compliance but, rather, reflect systemic deficiencies such that meaningful consent cannot be exercised in the context of today's digital environment.

6.1. The Limits of Behavioral Science on Consent

Consent-driven regulations are premised on the notion that individuals have sufficient information and independence to engage in rational decision-making regarding their own data as processed. Behavioral economics provides mounting evidence that, in fact, many decisions made by people regarding their own privacy and the use of their data will be made under conditions of bounded rationality characterized by a lack of time and/or cognitive capabilities [2].

Most individuals will be challenged to evaluate the many different ways that their data is being processed given the various and sometimes lengthy privacy notices, technical disclosures, and repeated requests for consent they have been confronted with on an ongoing basis. Thus, engaging in a meaningful way is less and less likely. Recent empirical research into the interfaces used for getting consent under GDPR reveals that people regularly give consent even if they do not fully understand what they are consenting to or the effects of that consent on the data processing [6].

Furthermore, "consent fatigue" threatens privacy governance. The constant barrage of requests for consent to track a user's behavior can lead some users to simply agree to tracking in order to access the content or continue using the service. At times, when consent is obtained under these conditions, the "consent" is just a matter of convenience and not informed agreement.

6.2. Privacy Paradox and Information Asymmetry

Another significant limitation to consent-based governance can be found in the so-called "privacy paradox," which is also referred to as the "privacy calculus" by privacy researchers and scholars. Although many individuals will openly express concern regarding the collection and/or use of their personal information, they will often not act on that concern, even though they continue to use online services, which are becoming impossible to avoid [34].

Thirdly, while organizations that collect data on users possess a tremendous amount of knowledge related to how they collect, profile and monetize users' data, users of online platforms are largely left to make decisions based on a limited amount of fragmented information [31]. As a consequence, implicit consent may be a matter of structural constraints rather than actual choices made by users.

6.3. Manufactured Consent and Dark Patterns

The use of dark patterns makes obtaining meaningful consent even harder. A dark pattern is a design strategy that intentionally alters user behavior on a website or application in favor of the organization providing the service. Despite being formally compliant with legal standards, consent interfaces are usually designed to encourage acceptance of the terms and conditions and discourage rejecting them.

Empirical research suggests that dark patterns are used widely. For example, Mathur et al. conducted a large-scale experiment analyzing 11,117 websites, and their results showed that websites frequently employ other techniques to manipulate users, such as obstructing access to information, framing information to be misleading, and creating asymmetric decision-making processes [35]. While studies on cookie consent (GPDR) continue to demonstrate similar issues, most websites still legally comply by providing clearly labeled "Accept All" consent options while making it more difficult for users to find or use a mechanism for refusing consent [17,36].

These manipulative consent practices can undermine the voluntary consent requirement of law and therefore the issues at issue are not simply whether users click the "Accept" button, or what the terms were for which consent was requested; rather, the conditions

under which consent was obtained also determine whether they are compatible with the fundamental principles of autonomy and self-determination that privacy regulation is intended to protect.

6.4. Regulatory Displacement and Technological Adaptation

The success rate of specific tracking technologies that can be reduced via legal means is minimal due to the evolution of the digital marketplace. The existence of consent-based governance in digital markets restricts success when you consider how rapidly these new forms of identification have emerged (such as server-side tracking and device fingerprinting), while third-party cookie use continues to decline as a result of regulation [3]. Although there are technical distinctions between these tracking tools and those used traditionally, from a functional perspective, these tracking systems enable similar forms of behavioral profile creation across different digital touchpoints.

The process by which technology-specific regulations can be evaded demonstrates fundamental limitations in the effectiveness of technology-specific regulations [14].

Organizations can comply with restrictions on specific tracking technologies but still engage in behavioral surveillance to a very similar extent using other means. Therefore, the real challenge lies not in whether or not a specific technology exists but instead in whether or not the data-driven business models will continue to create incentives for organizations to engage in high levels of behavioral surveillance.

6.5. Structural Failures of Consent

Overall, the indicated developments collectively demonstrate structural limitations within a consent-based regulatory regime. The presence of information asymmetries obstructs individuals' ability to make informed decisions about their use of technology; behavioral design techniques are designed to affect how users interact with technology; and the capacity for digital technologies to continue to exist and not be impacted by prior regulatory efforts demonstrates that users do not have meaningful control over their use of technology. Thus, in this environment, consent has increasingly been used as a mechanism for validating the extraction of data, rather than for limiting the extraction of data. The reliance on consent as the primary protection of privacy hides the deeper issues of the power of platforms, behavior manipulation and the inequality of information.

7. Towards a Rights-by-Default Framework: Informational Fiduciaries, Structural Privacy Protection

The previous section shows the limitations of current cookie governance in that consent-based frameworks cannot handle the imbalances in power, information and expertise that characterize digital markets. If you cannot get useful consent in places that are controlled by behavior manipulation and platforms having taken control of a substantial amount of personal information, privacy regulation needs to move away from models that focus on individual decision-making.

Information Fiduciary Theory is a well-known response to this issue. Specific platforms within the digital realm serve a fiduciary-like purpose because they collect, process and have a great deal of control over the personal information that users give them [7,8]. Just as the lawyer/client and doctor/patient relationships are characterized by dependence and informational imbalances, so is this interaction, and thus the need for a larger duty beyond ordinary contract obligations [37]. The importance of the fiduciary model is related to how it imposes different responsibilities on people and companies involved in providing digital services to their customers [38]. Instead of focusing on whether users provided valid consent prior to engaging in a particular practice, the focus moves to determining

if companies have carried out their duties of care, loyalty, and good faith towards those users [39,40]. Regarding the practice of behavioral tracking, this would include evaluating practices that involve the use of Dark Patterns, deceptive consent interfaces, and opaque profiling mechanisms, regardless of compliance with the technical requirements for obtaining consent.

Critics have expressed doubt about whether simply creating fiduciary obligations would be sufficient to regulate business models that depend on vast amounts of data being collected and used for the purpose of Behavioral advertising [41]. These issues point out that fiduciary duties should be part of a broader system of structural safeguards rather than a complete solution to regulating the collection, use and sharing of individuals' personal data.

Hence, this article recommends creating a rights-by-default framework that combines fiduciary obligations with nonwaivable privacy protections. Specifically, (1) data minimization should be used as an actual prohibition against collecting any data for which the company is unable to demonstrate that it needs to [9]; (2) purpose limitation needs to be applied in such a way that it does not allow companies to circumvent the regulation of behavioral profiling using other means of tracking [20]; and (3) all forms of behavioral manipulation should be treated as presumptively illegal whenever they result in a violation of an individual's ability to freely and meaningfully make choices [31,42]. A reformed view of the regulations in the area of privacy by law should be based on protecting a person's right to privacy, not just a consent-based model of privacy governance. This means the law should impose a minimum amount of privacy protection no matter how a person has agreed to give up their right to privacy; for example, under a standardized terms of use agreement or through manipulative design practices, etc. Thus, instead of viewing privacy as a contract option, the legal system would require that privacy exists as a basic legal right or as part of the law.

The goal is not to do away with consent altogether, but to acknowledge and be aware of the limitations of consent and to prevent the protection of your privacy from being solely based upon your choice made in a power- and knowledge-depleted environment.

The proposed framework does not suggest that consent has no regulatory value. Consent mechanisms can provide meaningful protection where users are presented with clear information, genuine alternatives, and interfaces that do not manipulate the exercise of choice. Technological privacy-enhancing measures, including browser-level controls, improved consent management tools, encryption, and data minimization technologies, may also complement legal safeguards by strengthening the practical ability of individuals to exercise control over their information. The concern is therefore not with consent as such, but with treating consent as a sufficient safeguard in circumstances where structural inequalities, behavioral manipulation, and complex data-processing practices substantially restrict the conditions necessary for autonomous decision-making. The implementation of a rights-by-default framework would nevertheless present practical challenges, particularly in defining the scope of non-waivable privacy rights, determining when data collection is genuinely necessary, and preventing regulatory uncertainty for organizations operating across jurisdictions. Such a framework would therefore require clear statutory standards, technology-neutral regulatory guidance, proportionate enforcement mechanisms, and periodic review to account for emerging forms of tracking. The objective should not be to prohibit legitimate data-driven innovation, but to establish a minimum level of privacy protection that cannot be displaced merely through contractual consent or technological adaptation. In this manner, structural safeguards can operate alongside individual choice rather than seeking to eliminate consent from privacy governance altogether.

8. Global Tracking/Digital Tracking Assessment

The Cookie laws and the regulatory mechanisms associated with the cookie laws are not unique or limited to a single jurisdiction. Each of the jurisdictions of the European Union, the United States, and India continues to face many of the same fundamental challenges related to cookie laws and regulatory systems. Consequently, cookie law and tracking will likely continue to face similar challenges across every region, country, governmental body or policy. The fact that the structural shortcomings of the consent-based regulation and governance of cookie laws will continue to hold true across jurisdictions suggests that shortcomings of consent-based governance are not unique to one jurisdiction, but rather are a result of structural limitations of their individual jurisdictions. Currently, there is a considerable disparity among different jurisdictions in their conceptualization and enforcement of privacy regulations. The European Union utilizes a rights-based framework that focuses on lawful processing and informed consent; the United States employs an approach based on consumer protection and market transparency, while the Indian data protection regime attempts to balance privacy rights with economic and development considerations through the use of a Data Fiduciary model [9,24,43]. While this may be true, it is noteworthy that some common principles are developing as they converge on the same key values, such as transparency, accountability, purpose limitations, and user control of personal data [19,44].

Moving forward, regulatory frameworks for regulatory developments must focus on harmonizing the underlying principles of governance rather than harmonizing with respect to specific technologies. Technology-based regulatory regimes will generally be obsolete when new methods of tracking can be created and used in the future, but technology-neutral regulatory frameworks will continue to have sufficient flexibility and adaptability for change over time within a digital environment. Principles such as data minimization, purpose limitation, accountability and fiduciary responsibility provide a more robust basis for privacy protection than regulatory requirements that are solely aimed at regulating specific types of tracking technology. A move away from disparate compliance models to unified baseline protections with the potential to operate across multiple jurisdictions could be advantageous for global privacy governance [9,20,45]. This wouldn't remove national regulatory disparity but could decrease regulatory arbitrage and enhance protection against behavior-based monitoring. Looking forward, the success of future digital privacy laws will depend less upon the legal means of consent and more upon developing structural safeguards to preserve individual autonomy within an ever-more data-driven world.

9. Conclusions

The transformation of cookies from mechanisms for maintaining web sessions into components of sophisticated behavioral tracking systems reflects a broader transformation in the digital economy: personal and behavioral information has become an important source of economic value. Privacy regulation has responded by placing substantial emphasis on individual consent through frameworks such as the GDPR, CCPA/CPRA, and DPDPA. However, the persistence of behavioral tracking demonstrates that formal consent mechanisms do not necessarily provide meaningful control over personal information when users operate within technologically complex and economically asymmetric digital environments.

The analysis demonstrates that the Consent Illusion arises from the interaction of several system-level factors. Information asymmetry limits users' understanding of data-processing practices; dark patterns and interface design can influence the exercise of choice; consent fatigue can reduce meaningful engagement; and technological substitution allows tracking practices to continue through alternative technical mechanisms. At the same time,

platform business models create strong economic incentives for the collection, analysis, and monetization of behavioral data.

These findings indicate that privacy governance cannot rely solely on the existence of a formal consent event. Consent has an important role within data protection law, but its effectiveness depends on the technical, informational, behavioral, and economic conditions under which it is obtained. A user clicking an "Accept" button does not by itself demonstrate meaningful informational self-determination when the user lacks practical knowledge of the processing architecture, faces manipulated interface choices, or cannot reasonably avoid the service.

The technical analysis of tracking technologies also demonstrates the limitations of technology-specific regulation. Restricting third-party cookies does not necessarily eliminate behavioral tracking when organizations can employ device fingerprinting, server-side tracking, or other functionally equivalent mechanisms [3]. The regulatory target should therefore move beyond individual technologies toward the underlying data-processing functions and behavioral surveillance practices that those technologies enable.

The principal contribution of this paper is the proposed Rights-by-Default Privacy Governance Framework. The framework combines fiduciary obligations, data minimization, technology-neutral purpose limitations, and protections against behavioral manipulation. Rather than making privacy protection dependent exclusively on an individual's ability to provide or withdraw consent, the framework establishes a baseline level of protection that applies before and beyond individual consent.

Within this framework, data minimization should operate as a substantive restriction on unnecessary collection [9]. Purpose limitation should be sufficiently technology-neutral to prevent organizations from circumventing restrictions on behavioral profiling simply by replacing one tracking technology with another [20]. Behavioral manipulation through dark patterns and similar interface practices should receive heightened scrutiny where it interferes with an individual's ability to make a free and meaningful choice [31,42].

The framework also incorporates the concept of information fiduciaries, recognizing that digital platforms possess substantial informational and technological power over users [7,8]. Fiduciary duties of care, loyalty, and good faith can complement conventional privacy obligations by shifting part of the regulatory focus from whether users formally consented toward whether organizations acted responsibly in exercising control over users' information.

However, fiduciary obligations alone are unlikely to resolve all structural problems. They should operate within a broader privacy architecture containing non-waivable minimum protections. The objective is therefore not to replace individual choice with unrestricted regulatory control, but to ensure that individual choice operates within a system that preserves a minimum level of informational autonomy.

The proposed approach consequently represents a shift from consent-centric privacy governance toward structural privacy governance. Under a consent-centric model, the principal regulatory question is whether an individual has provided legally valid consent. Under a structural model, the inquiry expands to include how data is collected, how tracking systems are architected, what purposes data processing serves, whether alternative tracking technologies circumvent regulatory restrictions, how interfaces influence decisions, and what obligations should apply to organizations controlling the relevant systems.

This approach is particularly important as digital tracking becomes increasingly distributed across browsers, devices, servers, advertising exchanges, analytics systems, platforms, and data intermediaries. Privacy regulation that focuses narrowly on one technical mechanism risks becoming obsolete as system architectures evolve. Technology-neutral principles such as data minimization, purpose limitation, accountability, fiduciary respon-

sibility, and protection against manipulative design provide a more adaptable basis for governing future tracking technologies [9,20,45].

The study is doctrinal and socio-legal rather than experimental and therefore does not empirically measure the effectiveness of the proposed framework. Future research should investigate how rights-by-default principles can be translated into technical privacy controls, including browser-level enforcement, privacy-preserving identity systems, automated detection of dark patterns, data-flow auditing, privacy-enhancing technologies, and machine-readable purpose and consent controls. Such research could provide a stronger technical foundation for implementing structural privacy protections within real-world digital platforms.

Ultimately, the Consent Illusion is not simply a problem with consent interfaces; it is a systems-governance problem. Meaningful informational self-determination requires more than giving users a button to click. It requires a digital environment in which data collection is proportionate, purposes are constrained, interfaces are not manipulative, tracking technologies cannot simply circumvent regulatory restrictions, and organizations exercising informational power remain accountable.

The future of digital privacy governance should therefore preserve consent while moving beyond consent as the sole protective mechanism. A Rights-by-Default approach can provide the structural foundation necessary to protect individual privacy within increasingly complex, data-driven digital ecosystems while still allowing legitimate technological innovation and responsible data use.

Author Contributions: Conceptualization, P.D.; methodology, P.D. and C.V.; software, P.S.R.; validation, A.M., A.G., A.R., P.S.R., P.D. and C.V.; formal analysis, P.D. and C.V.; investigation, A.M., A.G., A.R., P.S.R.; resources, P.D., C.V.; data curation, P.D.; writing—P.D., C.V.; writing—review and editing, P.D., C.V.; visualization, P.S.R., A.M.; supervision, P.D.; project administration, C.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are available in this manuscript.

Acknowledgments: The authors extend their sincere appreciation to Rishi Raj Bharadwaj for his invaluable advice, assistance, and insights throughout the research process. The success of this study can be attributed in great part to his knowledge and ongoing support throughout the course of this project. The authors also wish to thank Gaurav for his willingness to provide assistance, constructive feedback, and ongoing support throughout the research process. The authors are also thankful to their peers for their support through encouraging words, meaningful conversations, and collaborative efforts that greatly aided in the development of this paper. A special thank you is also given to the authors' parents for their unwavering support, patience, and motivation as the authors progressed through their education and completed their research work. The authors' parents have inspired them to pursue their academic and research goals. Finally, the authors wish to express their heartfelt thanks to Mahindra University, School of Law for providing them a forum and the resources and academic setting necessary to conduct and complete their research. The support and opportunities provided by the University have a profoundly positive impact on the authors' academic and scholarly success. The authors acknowledge, with appreciation, the contributions made by all individuals who have played a part in confirming the completion of their research project.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
DPDPA	Digital Personal Data Protection Act, 2023 (India)
EU	European Union
GDPR	General Data Protection Regulation (EU)
HTTP	Hypertext Transfer Protocol
IAB	Interactive Advertising Bureau (Europe)
SSRN	Social Science Research Network
US	United States

References

1. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; PublicAffairs: New York, NY, USA, 2019.
2. Acquisti, A.; Taylor, C.R.; Wagman, L. The economics of privacy. *J. Econ. Lit.* **2015**, *54*, 442–492. [CrossRef]
3. Englehardt, S.; Narayanan, A. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2016; pp. 138–146. [CrossRef]
4. Fu, L.; Zhang, J.; Wang, S.; Wu, X.; Wang, X.; Chen, G. De-anonymizing social networks with overlapping community structure. *IEEE/ACM Trans. Netw.* **2020**, *28*, 360–375. [CrossRef]
5. Utz, C.; Degeling, M.; Fahl, S.; Schaub, F.; Holz, T. (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 973–990. [CrossRef]
6. Zuiderveen Borgesius, F.J. *Improving Privacy Protection in the Area of Behavioural Targeting*; Kluwer Law International: Alphen aan den Rijn, The Netherlands, 2015.
7. Balkin, J.M. Information fiduciaries and the First Amendment. *UC Davis Law Rev.* **2016**, *49*, 1183–1234.
8. Balkin, J.M. The fiduciary model of privacy. *Harv. Law Rev. Forum* **2020**, *134*, 11–37.
9. Hijmans, H. The European Union as a Constitutional Guardian of Internet Privacy and Data Protection. Ph.D. Thesis, University of Amsterdam, Amsterdam, The Netherlands, February 2016.
10. *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände e.V.*; Court of Justice of the European Union: Luxembourg, 2019; Case C-673/17.
11. *AB Europe v. Gegevensbeschermingsautoriteit*; Court of Justice of the European Union: Luxembourg, 2024; Case C-604/22.
12. Banakar, R.; Travers, M. *Introduction to Theory and Method in Socio-legal Research*; Hart Publishing: Oxford, UK, 2005.
13. Bodie, M.T. Employers as Information Fiduciaries. *St. Clara Law Rev.* **2023**, *63*, 1–15.
14. Ayres, I.; Braithwaite, J. *Responsive Regulation: Transcending the Deregulation Debate*; Oxford University Press: Oxford, UK, 1995.
15. Turow, J.; King, J.; Hoofnagle, C.J.; Bleakley, A.; Hennessy, M. Americans reject tailored advertising and three activities that enable it. *SSRN Electron. J.* **2009**, *1478214*, 1–27. [CrossRef]
16. Ryan, J. *Action File: Real-Time Bidding (RTB) ad Auctions*; Irish Council for Civil Liberties Enforce: Dublin, Ireland, 2022. Available online: https://enforce.ie/rtb/ (accessed on 3 November 2026).
17. Santos, C.; Bielova, N.; Matte, C. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technol. Regul.* **2020**, *2020*, 91–135. [CrossRef]
18. Im, J.; Asthana, S.; Chen, Z.; Banovic, N. A large-scale analysis of user preferences in cookie banners. In Proceedings of the CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 11–16 May 2024; pp. 1–21.
19. Kranenborg, H.; Lynskey, O. The foundations of EU data protection law. *Int. Data Priv. Law* **2016**, *6*, 324–326. [CrossRef]
20. Kuner, C.; Bygrave, L.A.; Docksey, C.; Drechsler, L.; Tosoni, L. *The EU General Data Protection Regulation: A Commentary—Update of Selected Articles*; Oxford University Press: Oxford, UK, 2021.
21. De Hert, P.; Papakonstantinou, V. The new General Data Protection Regulation: Still a balanced instrument? *Comput. Law Secur. Rev.* **2016**, *32*, 345–375. [CrossRef]
22. *Justice K.S. Puttaswamy (Retd.) v. Union of India*; Supreme Court of India: New Delhi, India, 2017; Volume 10, p. 1.
23. Ahmed, S.; Nasir, M. Stakeholder perceptions of India's Digital Personal Data Protection Act of 2023: An empirical study across legal, banking, and corporate sectors. *Front. Sociol.* **2026**, *11*, 1753383. [CrossRef]
24. Matthan, R. *Privacy 3.0: Unlocking Our Data-Driven Future*; HarperCollins India: Noida, India, 2018.

25. Sengupta, A.; Hasan, F. *Writings on Indian Data Protection and Constitutional Privacy*; Vidhi Centre for Legal Policy: New Delhi, India, 2021.
26. Kumaraguru, P.; Cranor, L.F. Privacy Indexes: A Survey of Westin's Studies. CMU-ISRI-05-138; Institute for Software Research International, School of Computer Science, Carnegie Mellon University: Pittsburgh, PA, USA, 2005.
27. Chowdhury, N. Privacy and Citizenship in India: Exploring Constitutional Morality and Data Privacy. *NUJS Law Rev.* **2026**, *11*, 421.
28. Singh Sethi, M.I.; Manjunatha, N.; Channaveerachari, N.K.; Chakraborty, T.; Math, S.B.; Andrade, C. The Digital Personal Data Protection Act 2023: Implications for Mental Healthcare Practice in India. *Indian J. Psychol. Med.* **2025**, 1–6. [CrossRef]
29. Srnicek, N. *Platform Capitalism*; Polity Press: Cambridge, UK, 2017.
30. Cohen, J.E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*; Oxford University Press: Oxford, UK, 2019.
31. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*; Stanford University Press: Stanford, CA, USA, 2010.
32. Van Dijck, J.; Poell, T.; de Waal, M. *The Platform Society: Public Values in a Connective World*; Oxford University Press: Oxford, UK, 2018.
33. Khan, L.M. Amazon's antitrust paradox. *Yale Law J.* **2017**, *126*, 710–805.
34. Solove, D.J. The myth of the privacy paradox. *Geo. Wash. L. Rev.* **2021**, *89*, 1–51. [CrossRef]
35. Mathur, A.; Acar, G.; Friedman, M.J.; Lucherini, E.; Mayer, J.; Chetty, M.; Narayanan, A. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proc. ACM Hum.-Comput. Interact.* **2019**, *3*, 81. [CrossRef]
36. Bielova, N.; Litvine, L.; Nguyen, A.; Chammat, M.; Toubiana, V.; Hary, E. The effect of design patterns on (present and future) cookie consent decisions. In *Proceedings of the 33rd USENIX Security Symposium*; USENIX Association: Berkeley, CA, USA, 2024; pp. 2813–2830.
37. Balkin, J.M. The constitution in the national surveillance state. *Minn. Law J.* **2015**, *124*, 49–65.
38. Dobkin, A. Information Fiduciaries in Practice: Data Privacy and User Expectations. *Berkeley Technol. Law J.* **2018**, *33*, 1. [CrossRef]
39. Richards, N.M.; Hartzog, W. A duty of loyalty for privacy law. *Wash. Univ. Law Rev.* **2020**, *99*, 935–1013.
40. Richards, N.M.; Hartzog, W. Taking trust seriously in privacy law. *Boston Law J.* **2017**, *126*, 1180–1217.
41. Khan, L.M.; Pozen, D.E. A skeptical view of information fiduciaries. *Harv. Law Rev.* **2019**, *133*, 497–541.
42. Colloquium, E.V.P.D. *Theories and Models of the Privacy Paradox*; KIT Secuso: Karlsruhe, Germany, 2019; p. 951.
43. Solove, D.J.; Schwartz, P.M. *Fundamentals of Privacy Law*; International Association of Privacy Professionals (IAPP): Portsmouth, NH, USA, 2021.
44. Organisation for Economic Co-operation and Development. *The OECD Privacy Framework*; OECD Publishing: Paris, France, 2013.
45. González Fuster, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*; Springer International Publishing: Berlin/Heidelberg, Germany, 2014. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.