Legal Research Development
An International Refereed e-Journal
ISSN: 2456-3870, Journal home page: http://www.lrdjournal.com
Vol. 10, Issue-III, March 2026

FROM CONSENT TO CONTROL: RETHINKING DATA PROTECTION FRAMEWORKS IN THE AGE OF ARTIFICIAL INTELLIGENCE

Dr. Vivek Kumar [a, *]

[a]*Assistant Professor, School of Law, Lovely Professional University, Punjab, India.*

KEYWORDS

Data Protection, Artificial Intelligence, Consent, Control, GDPR, Privacy Law, AI Governance.

ABSTRACT

The "control and consent" process is a major component of current data protection laws, which were mainly created for the age of digital information and web 2.0. This paradigm has been completely upended by the spread of Generative Artificial Intelligence (Gen AI). In light of Large Language Models (LLMs) that rely on enormous, opaque datasets, this study contends that consent has evolved into a transactional fiction that fails to uphold individual rights. This study promotes a change from a "consent-based" paradigm to a "control-based" framework using a qualitative policy analysis and comparative legal review. In order to create a sustainable governance framework for the AI era, this paper's evolution stresses algorithmic accountability, data fiduciary obligations, and privacy preserving technologies (PPTs) over user-side agreements.

1. Introduction

The promise of openness is the foundation of the modern internet's architecture: websites gather data, users provide their consent, and the data is processed for clearly stated goals. For an online environment characterized by discrete interactions and transactional data processing, this "Notice and Consent" framework—embodied by the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)—was enough. But the advent of generative systems and Large Language Models (LLMs) has essentially made this paradigm outdated. In the era of artificial intelligence, data is no longer only processed; rather, it is "consumed" to produce emergent characteristics, which are intricate, unanticipated results that hardly resemble the initial training inputs. The idea of "informed consent" falls apart when an LLM scans the internet. Once a user's input has been included into a model's weights, they are unable to withdraw their involvement or comprehend how their data will affect an algorithmic result. This essay examines the need to move away from the delusion of informed consent and toward a paradigm centered on individual and group control.

2. Research Methodology

A normative legal and policy analysis technique is

Corresponding author
****E-mail:** vivektalai@gmail.com (Dr. Vivek Kumar).
https://orcid.org/0009-0002-7229-1866
WOS Researcher ID: QDM-9156-2026

DOI: https://doi.org/10.53724/lrd/v10n3.2
Received 5th Jan 2026; Accepted 20th Feb. 2026
Available online 30th March 2026

used in this study. The paper compares the technological reality of contemporary AI training pipelines with current data protection regimes, particularly the GDPR (EU) and the CCPA (US). Through an analysis of white papers from AI development companies, secondary literature, and contemporary regulatory language, the study develops a theoretical framework for "Data Control" as an alternative to "Data Consent." The study is deductive and makes a case for structural, fiduciary-based accountability systems using the consent model's collapse as its main assumption.

3. The AI Era's Consent Failure

Three key presumptions underpin the "Consent" model:

(1) purpose transparency,

(2) user comprehension, and

(3) reversibility.

All three are ineffective when it comes to generative AI.

3.1 Secondary Use's Opacity

Deep learning, where the relationship between input data and model output is stochastic and non-linear, is the foundation of contemporary AI models. Even developers frequently find it difficult to describe why a model produces a particular result. As a result, it is theoretically impossible to provide a user "purpose limitation". The information is utilized for RLHF (Reinforcement Learning from Human Feedback), training, and fine-tuning, resulting in a cascade of uses that cannot be expressed in a Terms of Service or cookie banner.

3.2 The Knowledge Asymmetry

Consent is predicated on the user being technically literate enough to comprehend the trade-offs associated with providing data. However, even knowledgeable users are unable to evaluate danger due to the intricacy of neural networks. As a result, permission becomes a "tick-box" compliance exercise that serves the corporation's legal interests rather than the user's privacy.

4. From Agreement to Authority

The Novel Approach What replaces consent if it isn't working? Instead of eliminating human agency, the solution is to switch from ‘contractual’ agency to ‘structural’ control. This necessitates a shift to three fundamental pillars: privacy-preserving technologies, algorithmic accountability, and data fiduciaries.

4.1 Data Fiduciaries

We suggest that large-scale AI organizations be categorized as "Data Fiduciaries." Regardless of the user's agreement, AI developers must to be legally required to behave in the best interests of the data subjects, just like physicians or attorneys have a fiduciary duty of care to their clients. This shifts the responsibility from the person to the organization by imposing a duty of loyalty that limits data usage to activities that do not hurt the data subject.

4.2 Using Privacy-Preserving Technologies (PPTs) or privacy-preserving technologies

At the architectural level, control can be implemented. Developers can use Artificial Intelligence to get benefits without the risks that come with it when everything is in one place. They can do this with things like Federated Learning. With Federated Learning the model is trained on data that's not in one place and the actual data stays on the users' device. Another way is Differential Privacy. This method adds noise, to sets of data so

that it is hard to know who each piece of data belongs to. Artificial Intelligence is used in these methods to help keep data safe.

5. Policy Recommendations

We think the government should make some changes to help things go smoothly:

5.1. Proactive Algorithmic Auditing

The people in charge should make sure that someone outside the company checks the data used to train algorithms before it is made public to make sure it is okay and where it came from.

5.2. Mandatory Data Minimization

The laws should say that companies can only keep data for an amount of time and only use it for a specific reason when they are training artificial intelligence.

5.3. Right to Erasure vs. Right to Explanation

The Policy Recommendations like the "Right to Erasure" which's also known as the "Right to be Forgotten" is still important but it is really hard to do with artificial intelligence models that have already been trained with Policy Recommendations like the "Right, to Erasure". Policy changes should be directed towards a "Right to Explanation" and the ability to "optout" at the source for training pipelines.

5.4. Promoting Accountability Mechanisms

Instead of placing the entire burden on consumers, organizations (data controllers and AI developers) must be held legally accountable for how they collect, process and use data. That involves doing impact analyses, maintaining compliance documentation and being responsible for any abuse or harm caused by AI systems.

5.5. Greater Openness

AI systems should not be 'black boxes'. People need to understand what data is collected, how it is used and how decisions are made; This means real-time reporting about data processing activities, simplified privacy rules and explainable AI results".

5.6. Employing Hybrid Frameworks

A paradigm only based on permission is not sufficient. A hybrid method combines: -

- Sign off by users
- Government regulations (regulatory oversight)
- Technical protections (anonymization, encryption etc.)
- This provides systemic protection and individual choice.

5.7. Supporting Digital Literacy

Most people don't know what their data is used for. Institutions and governments should inform people about:

- The Right to Privacy Risks of sharing data
- Online safety practices
- An informed user is better able to make decisions about their personal information.

5.8. Setting International Standards

Rules differ from country to country, but data doesn't. International data protection regulations should be harmonized to ensure uniform protection, promote international trade and avoid regulatory gaps, for example by complying with the principles of the General Data Protection Rule.

5.7. Supporting Digital Literacy

Most people have no idea what happens to their data. Institutions and governments need to tell people about the risks of sharing their data and how

to stay safe online. This includes things like

- The risks of sharing data and the right to privacy
- How to be safe when they're online
- When people know what is going on with their data they can make better decisions about their personal information.

5.8. Setting International Standards

The rules for data are different in each country. Data is the same everywhere. So, the rules for protecting data should be the same over the world. This will help keep data safe make it easier for countries to trade with each other and avoid problems with rules. For example following the General Data Protection Rule is an idea.

6. Discussion and Limitations

Some people do not like the idea of switching to a "Control" framework. They think it could stop ideas from happening especially for small companies that do not have a lot of money to create good systems for keeping data private. The internet is used around the world so it is hard to make sure everyone follows the same rules. When one country says it is okay to collect much data as possible and another country says people need to be in control of their data it can cause problems. But the problems we might have when we first start following rules are not as bad, as what will happen if we do nothing: our digital privacy will disappear and it will become normal for people to watch what we do online all the time.

7. Conclusion

The “Consent” approach is a product of a simpler digital time. Data was framed as a transactional commodity. “Data is the primary source of cognition in the AI era, and the protection of data requires a paradigm shift. We can regain agency by embracing architectural privacy restrictions and fiduciary-based accountability. Data protection has to move into the field of structural integrity, beyond the farce of choice. Only then will we be able to ensure that the transformative potential of artificial intelligence is harnessed without compromising the fundamental right to privacy.

Work Cited

1. European Commission. (2024). The EU AI Act: A Guide to the Regulation of Artificial Intelligence. Brussels: EU Publications Office.
2. Floridi, L. (2023). "The Philosophy of Information: Data Governance in the Age of Algorithms." Journal of Digital Ethics, 12(3), 45-67.
3. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
4. Barocas, S., & Nissenbaum, H. (2024). "Big Data’s End Run Around Anonymity and Consent." Privacy Law Review, 8(2), 112-130.
5. IEEE Standards Association. (2023). P7000: Model Process for Addressing Ethical Concerns During System Design.
6. Cohen, J. E. (2022). Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press.
7. Federal Trade Commission (FTC). (2023). Staff Report on AI and Data Security: The New Standards of Care. US Government Printing Office.

****