Page 667 - 676 **DOI:** *https://doij.org/10.10000/IJLSI.112672*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 3

2025

AI Exceptionalism and the Illusion of Control: India, EU, and the Global Crisis of Privacy

KABIR GABA[1]

ABSTRACT

This outline examines the global regulatory paradox surrounding artificial intelligence (AI) through the dual lenses of AI exceptionalism and the illusion of control. It critiques how privacy frameworks, particularly in India and the European Union, either delay intervention by overstating AI's novelty or rely on outdated consent-based models that fail to address AI's structural harms.

Employing a comparative, doctrinal, and policy-based methodology, the paper analyzes India's Digital Personal Data Protection Act, the EU's GDPR and EU AI Act, as well as international frameworks such as the OECD AI Principles and Article 19 standards.

Advocating for a post-exceptionalist model of governance, the paper calls for structural accountability, collective data rights, and democratic oversight. It reframes privacy not as an individual choice, but as a foundational condition for autonomy, equality, and public trust in the algorithmic age.

I. INTRODUCTION

The regulations surrounding AI are caught in a paradox—oscillating between extreme hype and regulatory apathy. On one side, *AI exceptionalism* sees AI as novel and complicated to control leaving a gap in policies. On the other, the *false sense of control* thinks current privacy rules—based on consent—are enough even though AI is mixed up in widespread data gathering and tracking. Both ways of thinking don't deal with the huge differences in knowledge and power built into today's AI systems.

This paper focuses on two main ideas:

- **"AI Exceptionalism**: The idea that AI has a unique ability to change things. People often use this belief to put off making rules saying we need to innovate or that things are too uncertain.
- **The Illusion of Control**: The outdated trust in individual approval and notification systems to manage privacy. This approach doesn't work well with how AI systems handle data in a big-picture forward-looking way."

[1] Author is a Student at Symbiosis Law School, Pune, India.

 [ISSN 2581-9453]

The literature work regarding AI and privacy is increasingly coming to the agreement that the classical frameworks built on consent and control from the individual's perspective have started failing in the context of algorithmic governance and surveillance capitalism. Foundational critiques by "**Solove (2024)[2] and Zuboff (2019)[3]"** make clear how the practices of datafication and predictive technologies have fundamentally altered the landscape, and notice-and-choice routines have become largely ritualistic. This is also captured in Viljoen's theory of "**Democratic Data,"** wherein privacy steps out of the liberal rights-based framework towards collective governance through Data Fiduciaries. Scholars like **Salomé Viljoen[4]** and **Margot Kaminski[5]** advocate for structural regulation and oversight grounded in risk, moving away from older approaches that focused on burdening users with responsibility.

In the same vein, Calo's[6] critiques of AI metaphors coupled with Kaminski's assessment of frameworks for regulating risk create gaps that connect individual harms with systemic opacity. Most importantly, while alerting against the creation of what they refer to as new legal silos **(the "Law of the Horse"),**[7] thinkers like Easterbrook defend terrain which contemporary scholars Balkin and Waldman embrace,[8] arguing in favor of delineating ethics and regulation of AI from human rights based norms. There are also tensions: While celebrating and critiquing GDPR for the proclaimed rights of the data subject within the EU, scholars argue that it overly relies on individual agency to the detriment of subject other operational rights.

These works collectively showcase the intellectual fault lines in AI privacy discourse between autonomy and automation, between the rights and risks thereby justifying the need for reframing post-exceptionalist approach like this paper proposes.

II. THE MYTH OF INDIVIDUAL CONTROL IN THE AGE OF AI

A. Epistemic Asymmetry: The End of Privacy as Self-Knowledge

Contemporary developments in AI technology, particularly in relation to large language models, neural networks coupled with real-time data processing, have shifted the balance of knowledge power in favor of institutions. The individual was previously deemed sovereign over their own information, relying on '**epistemic privilege'** for privacy; now AI has shifted

[2] Daniel J. Solove, Artificial Intelligence and Privacy, 77 Fla. L. Rev. 1 (2025).
[3] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019).
[4] Salomé Viljoen, A Relational Theory of Data Governance, 131 Yale L.J. 573 (2021).
[5] Margot E. Kaminski, Regulating the Risks of AI, 103 Minn. L. Rev. 1951 (2019).
[6] Ryan Calo, Robots as Legal Metaphors, 30 Harv. J.L. & Tech. 209 (2016).
[7] Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. Chi. Legal F. 207.
[8] Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 U.C. Davis L. Rev. 1149 (2018).

 [ISSN 2581-9453]

the paradigm. With technologies like pervasive computing and surveillance, deep behavioral profiling, and computers that 'know' individuals' more than the individuals themselves, AI reverses the paradigm.[9]

Kevin Macnish's description of surveillance as **"automated epistemic capture"** fits best—the deep identity-determining liberal idea of self is now shattered. We as humans have always preserved our identity, and are the distinction makers, now AI is asking us to give up on our identity. Macnish believes that surveillance isn't just watching from a distance. Instead, it's observing and capturing knowledge about someone by inferring truths from their past actions. Information asymmetry becomes even more frightening once inferential information is out of reach to individuals subjected to its control—who are governed all aspects of modern life, including but not limited to, credit score access, healthcare services, employment, and even predictive policing enabled by behavioral analytics.[10]

No, this isn't just an infringement of privacy; it's a radical shift of nationalism per se. Consent requires knowledge, combination of two makes supreme sovereignty. However, with newly bred modern not understanding how information is captured, interpreted, and acted on, there leaves no shards of foundation for existence of consent. What emerges is a data subject—not an agent.[11]

B. The Control Paradox: Agency in the Age of Automated Inference

Legal systems in various places—from India's proposed DPDP Act to the GDPR—depend a lot on ways to get consent. But these have become a pointless show. People are swamped with privacy policies they can't understand and too many notifications. As Daniel Solove and Ari Waldman point out, this fake sense of control makes people feel more helpless: they have to make choices they can't understand, and then get blamed when they're watched.

Rather than protecting people's right to control their data, these control methods just dump work on people moving the job of managing privacy from rule-makers and big companies to the people whose data is being used. This causes big problems with AI systems where complicated designs and hidden decision-making make things even harder to see. You can't handle something you can't even notice.[12]

---

[9] Kevin Macnish, *The Ethics of Surveillance: An Introduction* (Routledge 2018).
[10] Daniel J. Solove, *Understanding Privacy* (Harvard Univ. Press 2008). Ari Ezra Waldman, *Privacy's False Promise: How Law Fails When It Comes to Personal Data* (Cambridge Univ. Press 2021).
[11] Salomé Viljoen, A Relational Theory of Data Governance, 131 Yale L.J. 573 (2021), https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance.
[12] Nick Couldry & Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford Univ. Press 2019).

 [ISSN 2581-9453]

We need new ways to talk about this: we should say "data workers" and "controlled selves" instead of "users" and "consumers." Control isn't a tech feature anymore; it's fiction.

C. Collective Data and the Collapse of Individual Agency

Al systems do not operate on isolated data points but on patterns within populations. In the "inference economy," as Alicia Solow-Niederman frames it, the power of Al arises not from individual profiling but from statistical associations drawn across millions. The data of the many constructs the profile of the one.

This challenges the atomized subject in privacy law. If the harms of Al derive from collective O training datasets, how can individual rights be exercised? When inference is based on others' data, traditional opt-out or notice systems are structurally irrelevant. The law is regulating the wrong interface.

Scholars such as Salomé Viljoen propose a relational theory of data governance, treating data as a social artifact rather than individual property. This demands a shift from control to solidarity, from individual rights to democratic oversight of data infrastructures.

D. Control and the Dehumanization of Privacy

By far the most pernicious illusion of control in the age of AI is the **depersonalization of privacy**. When privacy can be reduced to an engineering challenge — one that is handled through toggles and settings and dashboards — it is stripped of its moral and social richness. It becomes transactional.[13]

Framing privacy as a menu of configurable options abstract from underlying power asymmetries, coercive architectures, whether certain data practices should exist in the first place. We have learned to live within the architecture of surveillance and simply negotiate terms.

This is not control. This is consensual subjugation, and it is where AI exceptionalism must be unraveled — not because AI is different, but because it reveals the cracks in our current paradigms

III. UNDERSTANDING AI EXCEPTIONALISM: A DANGEROUS REGULATORY SHORTCUT

A. In what ways does the concept of AI exceptionalism impound regulatory innovation and postpone fundamental change to architecture in international privacy law?

[13] Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die* (Wiley 2016)."

AI exceptionalism is the idea that AI is a sufficiently new, complex, or unpredictable technology that it cannot be governed by already-existing legal frameworks. These framing yields what one might refer to as "regulatory deferral"—the deferment of structural change on the grounds that the technology needs to be understood before governance can be attempted. This concept is built on marketing not technology; the mythology of AI raised to the highest order. Scholars including **Eric Siegel** have revealed this as a rhetorical ruse: **"AI is just a label. A strong brand, but an empty promise."** In fact, most of today's AI systems are using statistical pattern finding — not autonomous cognition. Their risk is not one from mystery, but scale, opacity and **lack of accountability.**

This myth, however, has **paralyzed regulators**. By casting AI as "exceptional," the legal system avoids confronting its real-world consequences—automated profiling, predictive surveillance, algorithmic discrimination. Legislators delay, fearing that premature regulation may "stifle innovation," while in truth, **lack of regulation empowers unchecked extraction**. The longer this exceptionalist stance persists, the more embedded AI becomes in **critical infrastructure, governance, and labor markets**, without any accompanying ethical scaffolding.

But this myth has left regulators frozen in place. By insisting that AI is "exceptional," the legal system ducks the question of its practical implications: automated profiling, predictive surveillance, algorithmic discrimination. Legislators defer out of fear that the wrong regulations "stifle innovation," but in reality, it is a lack of regulation that encourages unregulated extraction. And this exceptionalist position drags on while AI embeds itself in critical infrastructure, governance, and labor markets without any ethical scaffolding being built to underpin the radical restructuring occurring around us.

B. Why is a privacy regulation model based on individual control insufficient in the age of AI, and what opposing systemic solutions can rectify this lapse?

AI exceptionalism has an impact on privacy laws in a unique way. It goes hand in hand with—and strengthens—the **illusion of control** in current privacy systems. Instead of looking at basic ideas again many legal frameworks put more emphasis on **consent-based models**. These models don't have the ability to handle today's AI systems well.

Let's look at **India's DPDP Act, 2023**: it brings in new terms like "data fiduciary" and stricken consent rules, but it **states nothing about holding algorithms accountable--automated profiling, or AI-based inference-making**. At the same time, systems like "**Digi-Yatra**, **Co-WIN**," and **facial recognition used by authorities** rely on AI-powered profiling without real

public input, oversight, or ways to address concerns. In these situations, consent becomes **just a formality at best and forced at worst** leading to what some call **"consent fatigue."**

In the **EU**, the **GDPR** gives people certain rights (access, rectification, objection, erasure). But these rights assume people can spot problems and grasp how algorithms affect them. This doesn't hold true for **machine learning systems that work in hidden ways, with feedback loops and probability-based outputs**. Even Article 22 of the GDPR[14], which tries to put limits on automated decisions, doesn't apply in many cases and is hard to know that we have **foundation models** like ChatGPT.

This means the **illusion of control** still exists: laws give a sense of power, but real power lies with **designers, data scientists, and platform architects**. Privacy turns into a mere formality; individual rights are respected on paper, but **not in practice**.

C. How do India's DPDP Act and the EU's AI and Data Protection frameworks respectively mitigate or do not mitigate the systemic structural privacy risks inflicted by AI?

The paper suggests moving from **privacy models focused on individuals who choose to participate** to **approaches that govern structure for everyone**. This starts by **not treating AI as special**, not by downplaying AI's dangers, but by seeing these dangers as **magnified versions of digital governance issues we've faced for a while**.

To begin with, laws need to **change from fixing problems after they happen to one person to setting rules for how things are made from the start**. This includes:

- **Making it required to check how algorithms affect people** (like DPIAs),
- **Setting standards for explaining and writing down how models work**, and
- **Having outside groups check** to make sure things are fair, responsible, and don't discriminate.

Second regulatory frameworks need to adopt **relational and systemic perspectives** drawing inspiration from academics like **Salomé Viljoen**. She contends that data isn't just "yours" but comes into being through **social and institutional connections**. Her idea of **"Democratic Data"** highlights:

- **Public oversight groups,**
- **Collective data rights,**

[14] Regulation (EU) 2016/679, art. 22, 2016 O.J. (L 119) 1.

- And **fiduciary duties** that mirror legal obligations of care

D. Comparative Case Studies

Jurisdiction	Regulatory Approach	Key Instruments	Notable Issues	Examples
India	Consent-centric; lacks structural reform	IT Act, 2000; PDP Bill (withdrawn); DPDP Act, 2023	Consent overload, no AI regulation, no DPIAs, fragmented enforcement	Facial recognition in policing, Co-WIN vaccination portal, Digi-Yatra biometric boarding system
EU	Rights-based; risk-tiered regulation (GDPR + AI Act)	GDPR; Proposed AI Act; Charter of Fundamental Rights	Overreliance on individual consent; under-regulation of foundation models	DPIAs for high-risk processing, biometric use bans in schools and public spaces
USA & Others	Sectoral + enforcement-driven (FTC, state laws, China model)	FTC Act; CCPA/CPRA; China's Cybersecurity, Data, and AI regulations	Fragmented approach, inconsistent definitions, top-down control (esp. in China)	FTC v. Facebook (privacy violations), California AI regulations, China's mass facial surveillance

Table 2.1 : Comparative Case Studies between Jurisdictions

IV. HUMANS REDUCED TO DATA SUBJECTS: THE PRIVACY CRISIS REFRAMED

The widespread pervasiveness of AI systems has caused catalyzation shift in how people are seen by law and technology. People are no longer merely holders of rights. Instead, they're becoming "data subjects" - entities defined by their behavior, biometrics, and relationships. This part looks at how this change challenges the basic ideas of freedom, agreement, and respect in privacy law. It also suggests we should think of privacy as something that affects society and politics as a whole, not just as something individuals own.

A. Structural Power and Catalysis of Data Colonialism

Recent studies on *data colonialism* and *surveillance capitalism* show how personal data have become the raw material for a new type of extraction and control. Zuboff's idea of predictive extraction and the colonial frameworks that 'Couldry' and 'Mejias' describe demonstrate how AI tech serves as a tool for structural dominance. Systems that use ambient intelligence and computing everywhere chip away at an individual's *epistemic privilege* allowing others to know more about people than they know about themselves.

In this setup, gathering data isn't a passive or side activity—it happens all the time, looks ahead, and is set up this way. These system designs make individual consent for show and not useful in controlling the effects of widespread data use.

B. AI Environments Blur the Line Between Public and Private

AI erases the usual boundaries between public and private areas. Smart assistants, wearables, CCTV, and IoT networks always collect data from our most personal spaces. These tools don't just watch; they guess, deduce, and sort. As a result, our homes once thought to be private retreats now face non-stop monitoring.

Legal ideas like "reasonable expectation of privacy" find it hard to keep up with this flowing never-ending surveillance. This creates a new kind of person: the computer-processed human, whose self is shaped more by predictive grouping than by free will.

C. Seeing Privacy as a Shared and Systemic Benefit

Regular privacy laws based on personal control and individual freedom, struggle to handle widespread, AI-powered monitoring. People get tired of giving consent, face complex choices, and lack power making it hard for them to protect themselves.

Experts like Salomé Viljoen suggest we should see privacy as a *public good* similar to protecting the environment or public health. Her *Democratic Data* idea proposes that data handlers have responsibilities to users, people make decisions together, and everyone can join in making rules. This way of thinking makes privacy key to democracy and fairness, not just personal respect.

V. ROAD FORWARD: PRINCIPLES FOR A POST-EXCEPTIONALISM REGULATORY FRAMEWORK

A. Reconstructing Privacy Law on Systemic Foundations

The future of privacy regulation must shift away from reactive, individualistic paradigms. Structural obligations—such as purpose limitation, data minimization, and mandatory impact assessments—should be embedded into the development and deployment of AI systems. These obligations must address not just individual harm, but *systemic effects* like bias, exclusion, and epistemic injustice, which are often invisible within current regulatory approaches.

B. Regulating AI as Continuation, Not Exception

AI is not ungovernable—it is an evolution of existing digital governance challenges. Effective regulation requires adapting current legal frameworks rather than discarding them. Tools such as

algorithmic audits, explainability mandates, and oversight for automated decision-making should be integrated into data protection and anti-discrimination regimes.

This strategy avoids the pitfalls of *AI exceptionalism*, which defers accountability by treating AI as inherently novel. Instead, regulation must acknowledge the continuity of risks and the urgency of governance.

C. Comparative Models for Reform Global approaches offer instructive models:

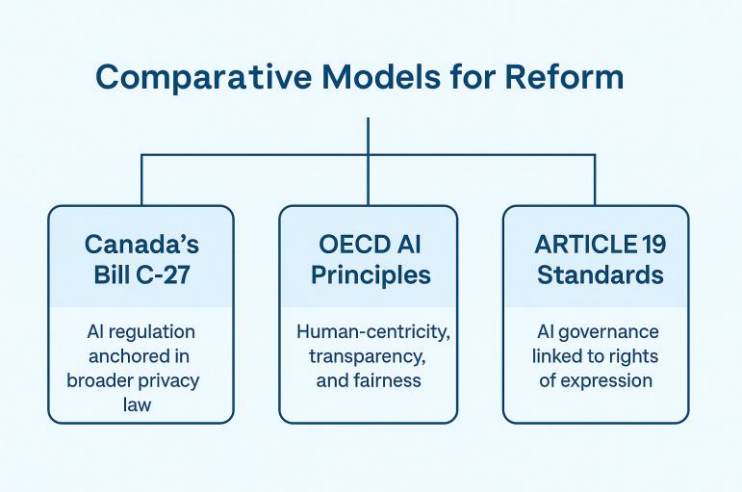

Table 3.1 : Comparative Models for Reform

VI. Conclusion and Personal Opinion

This research illustrates that **AI exceptionalism** is a distraction. Particularly in the context of privacy, considering AI as elusive from pre-existing regulations adds undue complexity such as **fragmentation, reactive, and ultimately ineffective** privacy frameworks like India's enforcement-by-consent model or the EU's over-burdened AI regulatory schemata. The core confusion lies within the belief that people retain the autonomy to manage AI's data utilization effectively.

Rather, privacy needs to be molded around a collectively shared construct strapped with societal guarantees, where informed consent becomes purposeless due to sophisticated algorithms, ambient CCTV systems, and perpetual data mining. A semantic change to the user being 'responsible' to the system being 'accountable' is what's paramount.

Personal Reflection

As a student of Law, I'd argue that describing AI as **un-regulatable** does not capture the reality—AI is **under-regulated technology**. The issue isn't technological, it's legal and political. Aimed at resolving nuanced problems AI policies need to integrate with existing frameworks enforcing algorithmic responsibility and understanding collective harms.

Relying on new technological tools to predict the future of privacy would be misguided, instead principles like **dignity, transparency, and justice** be applied boldly in the age of AI.

*****

 [ISSN 2581-9453]