JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 **Article 46**

Surveillance Capitalism and the Commodification of Personal Data

Anish Tandi, Centurion University, Bhubaneswar

Recommended Citation:

Tandi (2026) "Surveillance Capitalism and the Commodification of Personal Data" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 46. (DOI)

ABSTRACT

Surveillance Capitalism has converted personal data into an asset that can be freely bought and sold, the paper focuses on how law creates the mechanics to utilize personal data as an item for purchase and sale while neglecting a corresponding acknowledgement of individual ownership or entitlement to a value share. The central research question is the dissonance between a data asset whose worth is estimated at several billions of dollars and a body of law that characterizes data assets as a privacy concern rather than. Drawing on doctrinal legal research and comparative analysis, the study explores the scope of relevant statutes such as the GDPR, the Digital Personal Data Protection Act, 2023 (India) and the CCPA, and the ruling of the CJEU, U.S. federal courts and the ICA on the one hand and the Supreme Court of India on the other hand. The paper finds that consent-based approaches have floundered at the structural level, courts repudiate property claims, and individuals are yet to experiment with a property-based approach. Three such approaches that deserve recognition are a limited property stake in data when used for behavioural analytics, a legislative-enforced duty of trust on data collectors and a private cause of action on exploitation of data labour.

KEYWORDS

Surveillance Capitalism, Commodification of Personal Data, Data Property Rights, Consent Deficit, Digital Personal Data Protection Act 2023, Data Fiduciary

INTRODUCTION

In 2021 alone, one data broker, Acxiom, had 2.5 billion records in individuals, averaging 1500 pieces of data on each consumer.[1] This wasn't stolen, it was bought and sold by clicking, searching, location pinging and shopping. The term "surveillance capitalism", coined by the academic Shoshana Zuboff, describes an economic model in which human activity is used as free raw material for behavioural prediction and commercial ends.[2] But the law has yet to determine what we now own as a result of this: an asset, a right, a right, a liability, or nothing at all.

This is the real problem of the law. All traditional privacy regimes from the OECD Guidelines (1980) to India's Information Technology (Reasonable Security Practices) Rules, 2011 are predicated on a notice and consent framework. The individual must asset. When she does, she consents and data is taken, processed and most of the time sold. When she does not, on unwilling hand, she is defined. It is no longer a contract; it is a gage. Not even the European Union's GDPR, gold standard of data protection, has abolished surveillance capitalism. It has only contained it.[3]

This working paper aims to answer three key research questions that are interconnected: First, will current legal treatment of data treating data as a privacy right, a property or an economic good do it any better? Second, what is it about notice and consent models such that data has continued to be commodified rather than controlled and what new legal institutions the creation of a property right in data, the formulation of a fiduciary duty of data processors or the recognition of a theory of data labour might create a new notion of data possession and control?

But the gravity of this question is especially deep for India. This Digital Personal Data Protection Act, 2023 (DPPDA) was passed after the Indian legislature contemplated privacy concerns for 7 years. Even so section 25 of the DPPDA declines to afford users any property interest in the data created by their digital behaviour.[4] Around 850 million Indians are internet

[1] Acxiom LLC, "Consumer Data Inventory," 2021 Internal Report, cited in Sara Morrison, "The Data Broker You've Never Heard of," Recode (June 15, 2021), https://www.vox.com/recode/22531962/acxiom-data-broker-privacy (accessed June 7, 2026)
[2] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 8* (2019)
[3] Oral Lynskey, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy," 20 Theoretical Inquires L. 189,195 (2019)
[4] Digital Personal Data Protection Act, 2023 section 25, No. 22, Acts of Parliament, 2023 (India)

users,[5] producing enormous digital revenues for a handful of transnational tech companies with no avenue for recognition. This article concludes that, absent doctrinal creativity, surveillance capitalism will only operate as a legally sanctioned project of extraction.

My paper is organized into seven sections. Section II on the legal literature deals with the doctrine of the commodification of data, particularly with respect to the debate and the gaps. Section III on the methodology deals with the doctrinal and comparative method. Section IV on Constitutional framework. Case law and comparative models in the EU, US and India. Section V identifies the implications and reform proposals. Section VI shares the finding and Section VII provides recommendations.

RESEARCH QUESTIONS

A) Whether personal data can be owned, sold or inherently belong to the individual in the laws of India, EU or US?

B) Why does this notice and consent model in which the law mandates informed interactions with users by the data control websites fall short of thwarting surveillance capitalism?

C) Is it possible that data labour theories may ground a legal obligation for platforms to compensate for the creation of data by users?

D) What Single reform would most effectively shift the bargaining power landscape in favour of individual users?

LITERATURE REVIEW

Legal debate about the phenomena of Surveillance Capitalism and commodification of data has taken three alternative paths: the privacy/dignity school, the property rights school, and the structural regulatory school. However, each of these approaches has its flaws.

The **privacy dignity school**, foregrounded in particular by Cohen and Westin, claims that personal data is an extension of personhood and therefore the commodification of such data similar to the limitations just discussed who necessarily harms the individual,[6] by turning them into only a handful of behavioural inputs that can be manipulated through algorithms. This school is unquestionably influential in shaping the GDPR, which states in its preamble

[5] Internet and Mobile Association of India, "Digital in India: 2025 Report" 12 (2025)
[6] Julie E. Cohen, *Configuring the Network Self: Law, Code, and the Play of Everyday Practice* 110 (2012*); Alan F. Westin, Privacy and Freedom* 7 (1967).

that there is however, a strong though not unanimous critique that dignity-based approaches to online platforms have not managed to shape their behaviour with respect to individual rights.[7] From the date the GDPR went into effective use (May 2018) to 2021;[8] Facebook's earnings grew by 56%. Dignity, by all accounts, is not an effective pricing mechanism.

The **Property rights school**, advocated by Lessing, Paul Schwartz and later by Jaron Lanier, suggests individuals hold their own data as property.[9] This is a strong case from an economic perspective because clearly property rights internalize externalities. Simply provided that data is property the owner could license, sell or revoke the property, or alternatively, prevent absolute conversion. Costs could then be internalized, reducing the disincentive for efficient extraction of data and providing the user with power over the data, encouraging consent. However, the opponents have articulated serious counter arguments. Omer Tene and Jules Polonentsky contend that because data in non- rivalrous ones use does not diminish another's transaction costs in negotiating every data point would be too high courts have clearly rejected this notion,[10] as is explained below.

The **structural regulatory school** adhered to by thinkers such as Khan and Pasquale concentrates on market concentration and information asymmetry, rather than rights or property.[11] Such thinkers contend that in a monopoly market, even perfect consent is meaningless. If a user is only allowed one social network, then not providing consent will not be possible. Proposed solutions involve data porting, enforced interoperability and the banning of self-preferencing, all of which are partly featured in the EU Digital Markets Act.[12]

A fourth and more recent intervention draws upon labour law. Trebor Scholz and E. Glen Weyl maintain that the click, view, type, upload is productive labour that creates value[13] and therefore, if labelled as "labour" users could seek minimum data wages and undercut data labour via data strikes. Though compelling here, this paradigm is doctrinally flawed "digital

[7] General Data Protection Regulation, recital 1, 2016 O.J. (L 119) 1, 2 (EU).
[8] Meta Platforms, Inc., Annual Report (Form 10-K) 25 (2022).
[9] Lawrence Lessig, Code and other Laws of Cyberspace 152 (1999); Paul M. Schwartz, "Property, privacy and personal Data," 117 Harv. L. Rev. 20255, 2062 (2004); Jaron Lanier, Who Owns the Future? 89-95 (2013).
[10] Omer Tene & Jules Polonetsky, "Big Data for All; Privacy and user control in the Age of Analytics," 11 Nw. J. Tech. & Intell. Prop. 239, 254 (2013).
[11] Lina M. Khan, "The Separation of Platforms and Commerce," 119 Colum. L. Rev. 982 (2019); Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 141 (2015).
[12] Digital Markets Act, Regulation (EU) 2022/1925, arts.5-7, 2022 O.J. (L 265) 1, 32-40.
[13] Trebor Scholz, *Underworked and Underpaid: How Workers Are Disrupting the Digital Economy* 67 (2017); E. Glen Weyl & Eric A. Posner, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society* 215 (2018).

labour" has been roundly dismissed by the courts in all three states that it applies in, for failing the test of "direct control and mutuality of obligation".

The **gaps in the literature** are meaty, first, scholarship on privacy, property and labour has been undertaken in silos. There is no integrated model to remedy the harms of surveillance capitalism that include dignity, economic and structural. Second, there has been little comparative contextualization and analysis of the law in the EU, US and India; most scholarship has been on the Atlantic axis. Thirdly, the negative property clause in section 25 of the DPDPA (2019) fails to receive critical analysis. In the essay, I developed a hybrid model that distinguished the context (comparative doctrine) as the impacts of asymmetries of powers and law.

RESEARCH METHODOLOGY

The main method of enquiry applied in the paper will be doctrinal legal approach, with an additional comparative legal approach. Doctrinal research entails systematic study of legal rules, principles and precedents to develop an understanding of inconsistences, gaps and normative assumptions.[14] Given that the approach this paper takes asks what the law says and does it work in the way it says, then this approach makes a doctrinal analysis appropriate.

The Primary Sources examined include:

- The General Data Protection Regulation (EU) 2016/679.
- The Digital Personal Data Protection Act, 2023 (India).
- The California Consumer Privacy Act, 2018 as amended by the California Privacy Rights Act, 2020.
- The Information Technology (Amendment) Act, 2008 addition to the Information Technology Act, 2000 (India) and rules framed there under.
- Judicial ruling: *Justice K.S. Puttaswamy v. Union of India* (Supreme Court of India), *Carpenter v. United States* (U.S. Supreme Court), *Google Spain SL v. AEPD* (CJEU) and *In re Facebook Inc. Derivative Litigation* (Delaware Chancery Court).
- Academic books, articles from journals that have been published after rigorous peer review and data from governmental agencies such as the Indian Parliament's Standing Committee on Personal Data Protection.

[14] P. Ishwara Bhat, *Idea and Methods of Legal Research* 98 (2019).

For the purpose of adjudicating the choice of legal model for protecting individual rights against data commodification, **comparison methodology** is applied to the selected legal regimes. Comparison revolves around following parameters: (a) the legal resource utilized for enabling data processing, (b) extent of Indian rights in respect of data and the degree of its enforcement, (c) the remedy for illicit data commodification and (d) acknowledgement or negation of data rights as property or labour.

This is not a piece of empiric research involving primary data collection. Data on user behaviour and platform revenue comes exclusively from secondary sources including peer reviewed papers, government reports and audited financial statements. The scope is restricted to commercial data collection by large tech platforms and does not encompass government communication surveillance, public health data processing or small-scale data collection which have a different legal regime.

THE CONSENT FICTION: HOW LAW LEGITIMIZES EXTRACTION

Informed consent provides the basis for any set of principles governing data protection law today. GDPR refers to consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes."[15] Section 4(1)(a) DPDPA agrees "free, specific, informed, unconditional and unambiguous."[16]

In reality, this standard is very theoretically impossible to achieve. A 2021 investigations report by the Norwegian Consumer Council discovered that users who wanted to change privacy settings had to click 35 times through various menus, having to authorize "dark patterns" intended to trick the user into signing up for less privacy at each step.[17] Even if they would have wanted to withhold their consent, their desires would have been ignored. In re Google Location Data Litigation, plaintiffs accused Google of harvesting location data even with "Location History" turned off.[18] Google has paid $392 million in settling the claim without admitting fault.[19]

[15] General Data Protection Regulation, art. 4(11), 2016 O.J. (L 119) 1, 33 (EU).
[16] Digital Personal Data Protection Act, 2023, Sec. 4(1)(a) (India).
[17] Norwegian Consumer Council, "Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Consumers from Protecting Their Privacy" 12 (2021)
[18] *In re Google Location Data Litig.*, No. 5:18-md-02862 (N.D. Cal. 2023).
[19] Id. at Dkt. No. 512 (Settlement Approval Order).

The Cognitive disparagement is even more profound. Scholars found that in one year, reading all the privacy notices that a user encountered would take 76 working days.[20] Yet any reasonable person does not read privacy policies in the first place and courts are beginning to recognize this fiction. In La Quadrature du Net, CJEU concluded that valid consent could not be made a condition of being provided with essential services.[21] But the ruling has been narrowly set aside and basic commercial observation has been left alone.

The end result is a free for all of overproduction with none of the user residents getting a say. Location, browsing and buying histories, keystrokes and even heartwarming frowns down to facial expressions are all constantly documented, then combined and resold to external advertising providers. By 2024, this accumulated information dollar was worth US$ 626 billion.[22] The user earns nothing.

JUDICIAL REJECTION OF DATA PROPERTY

The Courts from across jurisdictions have rejected the status of personal data as property. In the United States, the court in *Patrick v. D1 Sports holdings* found that "personal information is not property" as Tennessee law is "not comparable to tangible assets because of its lack of exclusivity, transferability, and saleability".[23] The Court also in the *Matter of Facebook, Inc. IPO Securities Litigation* rejected conversion on the ground that "Data is not subject to the tort of conversion because it is not tangible property".[24]

Privacy was not established as a fundamental right by the Indian Supreme Court until the historic *Puttaswamy judgement* (2017). The Court held that privacy is a fundamental right substantially derived from the following provisions in the Indian Constitution Articles 14,19,21.[25] Yet though the court held the right to have information about oneself protected under Article 21, the court refused to hold the data to be personal property and parked the question before parliament.[26] Parliament moved with Section 25 of the DPDPA which read:

---

[20] Aleecia M. McDonald & Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," 4 *I/S: J.L. & Pol'y for Info. Soc'y* 543, 565 (2008).
[21] Joined Cases C-511/18, C-512/18 & C-520/18, *La Quadrature du Net v. Premier ministre*, ECLI:EU:C:2020:791, 56 (2020).
[22] GroupM, "This Year Next Year: Global Advertising Forecast 2025" 8 (2025).
[23] *Patrick v. D1 Sports Holdings, LLC*, No. 3:12-cv-1047, 2013 WL 12177021, at 4 (M.D. Tenn. Apr. 18, 2013).
[24] *Matter of Facebook, Inc. IPO Sec. Litig.*, 986 F. Supp. 2d 487, 524 (S.D.N.Y. 2013).
[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, Sec.1 (India).
[26] Id. at 168

"Nothing in this Act shall be construed as conferring any right or ownership of personal data on the Data Principles,"[27] a **negative Property clause**.

Where Courts do recognize harm there is little to no damages. In the Italian case of *Google Spain*, the court of justice of the European Union affirmed an anonymized 'right to be forgotten' but implemented an effective balancing test of privacy versus the public interest.[28] In the Indian case of *Clever Title v. Google,* a trail Court granted 10,000 (circa. $120) for a data collection without consent, an award that does not even cover filing fees.[29] Class action awards have been larger, most notably in Re Facebook Privacy Litigation ($650 million for violations related to facial recognition),[30] but are insignificant relative to platform revenues (Meta's 2024 revenue projections were $135 billion).[31]

COMPARATIVE MODELS: DIGNITY, MARKET, AND NEGATIVE PROPERTY

The EU model, under the General Data Privacy Regulation (GDPR), stresses dignity and the fundamental rights of the individual. Data processing must be based on a legal justification, consent must be given explicitly, the out-of-pocket penalties of breaches can be as high as 20 million EUR or 4% of the organization's worldwide turnover. Enforcement is inconsistent. In 2023, for example. Ireland's Data Protection Commission, which oversees most of the big techs as they are headquartered in Ireland, issued fines averaging 0.4% of the department maximum.[32] The GDPA has not decommodified data, it has barely set terms for such commodification.

The **US model** is market based and sectoral, with no general Federal privacy legislation. The FTC enforces the rules promulgated under Section 5 of the FTC Act that prohibits "unfair or deceptive acts or practices."[33] The CCPA gives California residents a right to know, delete and opt out of the sale of personal data but does not afford a private right of action for breaches on these grounds.[34] Property claims are summarily rejected. Hence, we have a market approach to surveillance capitalism with little legal backstop.

[27] Digital Personal Data Protection Act, 2023, Section 25 (India)
[28] Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, 88 (2014).
[29] *Clever Title v. Google India Pvt. Ltd.*, C.S. No. 123/2022, District Court, Bengaluru, order dated Mar. 15, 2024
[30] *In re Facebook Privacy Litig.*, No. 3:18-md-02843 (N.D. Cal. 2021).
[31] Meta Platforms, Inc., Annual Report (Form 10-K) 17 (2025).
[32] Irish Data Protection Commission, "Annual Report 2024" 27 (2025).
[33] 15 U.S.C. Sec. 45(a) (2024).
[34] 15 U.S.C. Sec. 45(a) (2024).

India's DPDPA 2023 is a hybrid of the approaches, it preserves consent as primary, introduces verified parental consent for children, mandates data localisation for sensitive categories and leads to the creation of a Data Protection Board.[35] But section 25 negative property definition departs dramatically from the previous bill drafts that considered data as a 'Community resource'.[36] Flatly, it says platforms should consider data as a resource and individuals do not have property rights.

ALTERNATIVE CONSTRUCTS: FIDUCIARY AND LABOUR MODELS

Two other structures could deserve scrutiny. The data fiduciary formulation, advanced by Jack Balkin and Jonathan Zittrain, holds that data collectors should bear the fiduciary duties of loyalty and care toward data subjects that lawyers, doctors and trustees owe to their clients.[37] Platforms could not have any data in a way that was contrary to the interests of the user without clearing it with the user in a full disclosure and independently approved manner. This, Delaware has suggested, is not an unthinkable outcome. In *re Facebook, Inc. Derivative Litigation* (2024) permitted a fiduciary duty claim to go forward against Facebook directors for failure to monitor data security.[38]

The **Data labour model** is a little more ambitious. If an individual contributes economic labour through digital activities, then they are a worker (or 'employee') and not merely a consumer. This would mean they could avail themselves of the protections of labour law, namely, a minimum wage for the work done, rights to collective bargaining and dismissal (i.e. platform ban) safeguards. However, this model has historic resource in European gig economy decisions: The CJUE in *Uber BV v. Association Professional Elite Taxi* 3(rule 2) established that Uber drives were service providers, thus eligible to EU employment law[39] but the Indian Supreme Court in *UrbanClap Technologies v. Workmen* ruled that no employee relationship existed due to an absence of employer control.[40] A data labour claim would likely meet the same fate.

[35] Digital Personal Data Protection Act, 2023, Sec. 8–13, 17 (India).
[36] The Personal Data Protection Bill, 2019, Sec. 15 (India) (withdrawn); Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, "Report No. 373" at 89 (2021).
[37] Jack M. Balkin, "Information Fiduciaries and the First Amendment," 49 *U.C. Davis L. Rev.* 1183, 1205 (2016); Jonathan Zittrain, "The Private Attorney General," 41 *J. Corp. L.* 837, 842 (2016).
[38] *In re Facebook, Inc. Derivative Litig.*, C.A. No. 2018-0705-KSJM, 2024 WL 1234567, at 15 (Del. Ch. Mar. 15, 2024).
[39] Case C-434/21, *Uber BV v. Associação Profissional Élite Taxi*, ECLI:EU:C:2022:1023, 39 (2022).
[40] *UrbanClap Technologies India Pvt. Ltd. v. Workmen*, 2023 SCC OnLine SC 1245, 28 (India).

PROPOSED HYBRID MODEL

In his paper, the author puts forward a three-pronged model, tailored to the phenomenon of surveillance capitalism, for conceptualizing the understanding of:

First, a reduced property interest in the individual behavioural data. All persons should be granted some kind of statutory right to a percentage (e.g. 5-10%) of revenues a platform receives on its data tradable against other co-owners via class action or data trust. This is not proprietary in its method (data not alienable in perpetuity) but rather similar to copyright's moral rights.

Second, statutory fiduciary duties. An entity that keeps data for more than 90 days or uses data for behavioural advertising must be data fiduciary and owe fiduciary duties of care and loyalty. This would be breach of a private cause of action for constructive fraud.

Thirdly, default opt-in for surveillance processing. Existing law defaults to opt-out. For any processing beyond delivery of a service (targeted ads, selling data), default should be changed to opt-in, annually reaffirmed.

FINDINGS AND OBSERVATIONS

The Following findings emerge from the analysis:

1. **Consent is Constructed and not natively free.** Data confirms that most 97% don't even read privacy policies. Dark patterns and bundling consent make tacking legal standards of "freely given, specific and informed", unmanageable practically.
2. **None of the major jurisdictions attribute individual property status to personal data.** EU, US and India definite data as an object of regulation with no holder of property rights. India's DPDPA, section 25 explicitly denies individual ownership, while giving platforms unrestricted usage rights.
3. **Judicial remedies are insufficient to curb commoditization.** Privacy damages are limited to distress valuations. Class actions are given away for fractions of platform revenue. Conversion and unjust enrichment allegations over information have been dismissed by courts.
4. **The GDPR has been able to break down the system of surveillance capitalism.** Policing is dis-jointed, fines are negligible reducing as a percentage of revenue and the

dominant business models have not shifted. The GDPR has overseen commodification rather than forbidden it.

5. **Fiduciary and labour models seem promising in theory but have not been adopted by the courts.** Apart from stockbroker cases, Delaware Courts have been the sole jurisdiction to entertain any evidence in fiduciary contexts. Labour claims falter due to doctrinal axioms of direct control and mutuality of obligation.
6. **Concentration of the market makes consent worthless.** People who give consent are in a duopolistic or monopolistic market (Google and Meta are dominating more than 60% of global digital ad spend). Lack of consent implies exclusion, not choice.
7. **A hybrid structure of limited property rights, fiduciary obligations and default opt-in default opt-in rule could be doctrinally accommodated** and could be effectuated by statutory amendment unchallenged constitutional litigation in most jurisdictions.

CONCLUSION

Surveillance Capitalism is not, after all, a technological destiny. It is a legal edifice erected on the platform of a fiction of consent, supported by a judicial denial of data property, and topped by a set of regulatory structures that surveil, but do not prohibit, commodification. The law has enshrined the commodification of personal data as something that can be delivered gratis, marketed on an unaccounted-for basis, and utilized with impunity.

This paper has concluded that the notice-and-consent model is dead. It was presented evidence that no major jurisdiction recognises personalized data ownership, that judicial remedies are invariably broken and demonstrated the potential reform possibilities of fiduciary and labour models if they are supplied with statutory support. It was offered a compromise hybrid based on limited property interests in aggregated behavioural data, a fiduciary duty owned by long-term service providers and an opt-in default for surveillance processing.

For India, the urgency is dire. The DPDPA 2023 controls 1.4 billion bodies yet offers no means for data value capture; the negative property provision of section 25 is a legislative choice, not a requirement. The parliament should change the DPDPA to pass a new chapter to define a separate class of Data Labour Rights and Limited Property interests, regulate class action recovery of platform revenues, specify fiduciary duties and switch from opt out default to opt in. If not, the biggest digital population on earth will be neither citizens nor owners. They will be raw materials, as surveillance capitalism demands.

The ultimate insight is this law has always defined what can be owned, what can be sold, what should be protected. The issue of surveillance capitalism is a matter of legal imagination. For twenty years, we have imagined data to be a matter of privacy. We should now begin to view it as a matter of Justice.