# THE DATA-EXTRACTION ECONOMY AND THE EROSION OF FUNDAMENTAL RIGHTS: A CRITICAL ASSESSMENT OF SURVEILLANCE CAPITALISM

Priyam Pratik, Faculty of Law, University of Allahabad

**ABSTRACT**

The contemporary digital economy has given rise to a form of accumulation that extracts value not from labour or natural resources, but from human behaviour itself. Surveillance capitalism, a term coined by Professor Shoshana Zuboff, describes a system in which personal data is harvested at scale, converted into predictive behavioural profiles, and monetised through targeted advertising and related commercial activities. This article critically examines the structural tension between surveillance capitalism and fundamental rights protections across multiple jurisdictions, with particular reference to the European Union, India, and the United States. Through an analysis of landmark case law including K.S. Puttaswamy v. Union of India (2017), Schrems II (2020), Carpenter v. United States (2018), and the CJEU's Google Spain ruling (2014), the article maps the evolving judicial and legislative responses to the encroachment of data-driven commerce upon rights of privacy, autonomy, dignity, and freedom of expression. The article identifies significant lacunae in the current regulatory architecture, including the commodification of consent, inadequate enforcement mechanisms, and the asymmetric informational power that technology corporations exercise over individuals. It further evaluates the Digital Personal Data Protection Act, 2023 (India), the GDPR regime, and the EU AI Act as partial but insufficient responses to this structural problem. The article concludes with constructive recommendations for a rights-anchored regulatory model that treats data sovereignty not as a market instrument but as a precondition of democratic freedom.

**Keywords:** Surveillance Capitalism, Fundamental Rights, Data Protection, GDPR, DPDPA, Privacy, Behavioural Data, Digital Economy, Informational Autonomy, AI Regulation.

## I. INTRODUCTION

Every time a person uses a search engine, taps a navigation app, or scrolls a social media feed, data is generated. That data does not disappear. It is collected, processed, cross-referenced with other data, and eventually transformed into something commercially valuable: a behavioural profile capable of predicting what a person will buy, believe, or vote for. This is the basic machinery of surveillance capitalism, and it operates largely beyond the sight of the individuals whose lives it catalogues.[1]

The term was introduced into academic discourse by Professor Shoshana Zuboff of Harvard Business School, who described it as the unilateral claiming of private human experience as free raw material for translation into behavioural data.[2] These data are then packaged as prediction products and sold into what Zuboff calls 'behavioural futures markets,' where the commodity on offer is not a product but a probability. The buyer is typically an advertiser; the subject of the transaction is you.

What makes this arrangement legally and philosophically troubling is not merely the scale of data collection, but its relationship to fundamental rights. Privacy, autonomy, dignity, and freedom of expression are not abstract philosophical commitments. They are enforceable rights guaranteed under constitutional instruments and international human rights frameworks across the world. And yet the architecture of surveillance capitalism routinely encroaches on each of these rights, often with the veneer of contractual consent offered through impenetrable terms of service.[3]

This article proceeds in six parts. Part II surveys the mechanics of surveillance capitalism and its economic logic. Part III analyses the fundamental rights engaged by that logic. Part IV examines key judicial developments across three jurisdictions. Part V compares the principal regulatory responses, identifying their strengths and gaps. Part VI identifies the lacunae that remain unaddressed, and Part VII offers constructive recommendations for a rights-anchored framework adequate to the challenge.

[1]SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 8 (PublicAffairs 2019).
[2]*Id.* at 11–12.
[3]Shoshana Zuboff, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, 30 J. INFO. TECH. 75, 76 (2015).

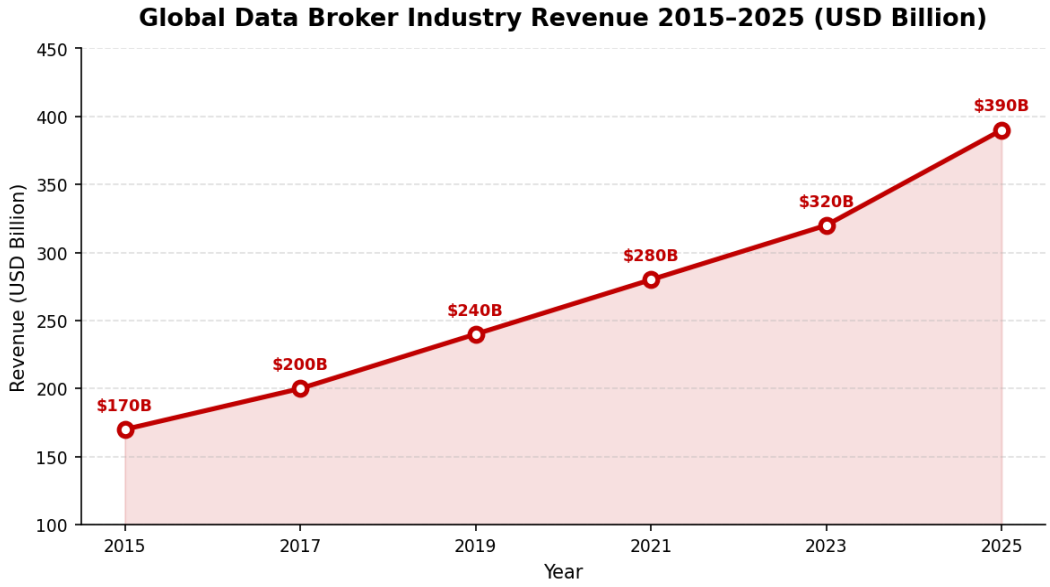
## II. THE ARCHITECTURE OF SURVEILLANCE CAPITALISM

### A. From Industrial to Behavioural Capital

Capitalism has always expanded by bringing new domains within the logic of the market. Industrial capitalism enclosed the commons and treated nature as raw material. Surveillance capitalism applies the same enclosure logic to human experience itself.[4] What once remained inside the private sphere, namely where one goes, what one reads, whom one loves, how one feels, has become a resource to be mined, quantified, and sold.

The proximate origin of this model lies with Google's discovery, around 2001, that the surplus data generated by its search users, data beyond what was necessary to improve the search service, could be used to generate extraordinarily accurate predictions about user behaviour. Advertisers were willing to pay a premium for those predictions. A business model was born.[5] Facebook, Amazon, and a growing ecosystem of data brokers, health apps, and smart devices have since extended that model into nearly every dimension of daily life.

The data broker industry alone was generating revenues of approximately $320 billion annually by 2023, with projections exceeding $390 billion by 2025. The chart below reflects this trajectory.




[4]ZUBOFF, supra note 1, at 93–94.
[5]Alessandro Acquisti, Curtis Taylor & Liad Wagman, The Economics of Privacy, 54 J. ECON. LITERATURE 442, 445 (2016).

*Figure 1: Global Data Broker Industry Revenue Growth, 2015-2025 (USD Billion). Source: Industry estimates.*

### B. The Behavioural Surplus and Predictive Power

The distinctive feature of surveillance capitalism is what Zuboff calls the 'behavioural surplus': data collected in excess of what a service requires for its stated purpose. A mapping application, for instance, may need a user's location to provide directions. It does not need to retain that location history indefinitely, correlate it with purchase history, and resell the combined profile to an insurance company. Yet this is routine practice. The surplus is precisely what gives surveillance capitalists their commercial advantage: the ability to predict, and ultimately shape, consumer behaviour.

The predictive power achieved through this data accumulation is formidable. Research associated with Cambridge Analytica's methods suggested that psychological profiles constructed from social media data could predict personality traits with accuracy exceeding that of a person's spouse after just a few hundred data points.[6] When that predictive capability is deployed in a political campaign, as it was in the 2016 United States presidential election and the Brexit referendum, the implications for democratic self-governance become acute.

### C. The Cambridge Analytica Inflection Point

The Cambridge Analytica scandal, which emerged publicly in March 2018, crystallised for a global audience what data researchers had long understood. The political consultancy had harvested the personal data of approximately 87 million Facebook users, mostly without their knowledge, through an application that exploited Facebook's Open Graph API to collect not only the data of app users but also the data of their friends.[7] That data was used to build psychographic profiles for political micro-targeting in the 2016 US election campaign.

The scandal drew legal consequences on multiple fronts. Facebook paid a $5 billion fine to the US Federal Trade Commission, then the largest in that agency's history for a privacy violation.[8]

---

[6]VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* 152–53 (Houghton Mifflin Harcourt 2013).

[7]Huntress, Facebook-Cambridge Analytica Data Breach: What Happened, Impact, and Lessons, https://www.huntress.com).

[8]CNBC, Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal (Apr. 10, 2018), https://www.cnbc.com.

More broadly, the episode illustrated a structural vulnerability: the consent framework underpinning social media data collection was fragile to the point of meaninglessness. Users had technically 'consented' to the app's terms; they had not meaningfully consented to the geopolitical use of their psychological profiles.

## III. THE FUNDAMENTAL RIGHTS DIMENSION

### A. The Right to Privacy

Privacy is the threshold right at issue in any serious engagement with surveillance capitalism. It encompasses not only freedom from observation but the deeper interest in controlling the narrative of one's own life: what information about oneself is known, by whom, and for what purpose.[9] This multi-dimensional conception of privacy was affirmed with unusual breadth by India's Supreme Court in K.S. Puttaswamy v. Union of India, decided by a nine-judge bench on 24 August 2017.

The Puttaswamy court unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution of India, overruling earlier decisions in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1963) that had denied constitutional protection to privacy.[10] Justice D.Y. Chandrachud's concurring opinion is especially significant for data protection: it identified informational privacy as a dimension of the right to privacy and recommended that the Government of India establish a robust framework for data protection.[11]

In the European Union, the right to privacy and the right to the protection of personal data are separately enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The GDPR operationalises these constitutional rights in a detailed legislative framework built around principles of purpose limitation, data minimisation, and accountability.[12] The United States, by contrast, does not have a comprehensive federal privacy right. Fourth Amendment jurisprudence has historically relied on the 'third-party doctrine,'

[9]HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 127–28 (Stanford Univ. Press 2010).
[10]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[11]*Id.* (Chandrachud, J., concurring).
[12]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) art. 4(1), 2016 O.J. (L 119) 1.

under which information disclosed to any third party loses constitutional protection, a doctrine increasingly ill-suited to the digital age.

### B. Autonomy, Dignity, and the Freedom to Choose

Privacy's relationship to autonomy and dignity is not merely philosophical. When a platform assembles a detailed behavioural profile of an individual and uses it to manipulate that person's choices through targeted content, it encroaches on the individual's capacity for self-determination.[13] The choice presented to the user is not a genuine choice in any philosophically meaningful sense: it is a choice already shaped, at the margins, by information asymmetries that the user cannot see and that the platform has deliberately maintained.

This concern sits at the heart of the concept Zuboff calls 'Big Other,' a distributed architecture of behavioural modification that operates without the crude visibility of the authoritarian state but may be, in its ultimate effects, more thoroughgoing in its restructuring of human agency. The state coerces; the platform nudges. But the nudge, calibrated to each individual's revealed preferences and psychological vulnerabilities, may be more effective than the coercion.

### C. Freedom of Expression and Epistemic Autonomy

Surveillance capitalism also intersects with freedom of expression in ways that are not always immediately obvious. Platforms that deploy recommendation algorithms to maximise engagement do not merely deliver content neutrally: they systematically promote content that provokes strong emotional responses, because such content generates more engagement data.[14] The result is the well-documented 'filter bubble' phenomenon: users are progressively exposed to content that confirms and radicalises existing beliefs, while content that challenges those beliefs is algorithmically deprioritised.

This structural distortion of the information environment carries implications for democratic deliberation that go beyond the conventional concerns of free speech law. The issue is not that speech is suppressed; it is that the commercial logic of surveillance capitalism systematically deforms the epistemic commons on which democratic self-governance depends.

---

[13]ZUBOFF, supra note 1, at 202.
[14]FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* 58 (Harvard Univ. Press 2015).

## IV. JUDICIAL DEVELOPMENTS: A COMPARATIVE ANALYSIS

Courts across jurisdictions have increasingly been called upon to adjudicate the tension between the commercial imperatives of the data economy and the fundamental rights of individuals. The following table summarises the key cases discussed in this Part.

***Table 1: Key Case Laws on Surveillance Capitalism and Fundamental Rights***

| Case | Forum / Year | Key Issue | Significance for Surveillance |
|---|---|---|---|
| K.S. Puttaswamy v. Union of India | Supreme Court of India, 2017 | Right to privacy as fundamental right under Art. 21 | Laid constitutional foundation for data protection; anchored informational privacy as a subset of the right to life |
| Google Spain SL v. AEPD | CJEU, 2014 | Right to erasure / right to be forgotten online | Established that search engines are 'controllers'; recognised individuals' rights to de-index personal information from commercial platforms |
| Data Protection Commissioner v. Facebook Ireland (Schrems II) | CJEU, 2020 | Validity of EU-US data transfers under surveillance-heavy US law | Invalidated the EU-US Privacy Shield; confirmed that commercial transfers cannot override fundamental rights to privacy |
| Carpenter v. United States | US Supreme Court, 2018 | Government access to cell-site location data without a warrant | Recognised that prolonged digital tracking requires Fourth Amendment protection; limited the third-party doctrine in the digital age |
| Meta Platforms Ireland Ltd. (GDPR Fine) | Irish DPC / EDPB, 2023 | Systemic EU-US data transfers without adequate safeguards | Record EUR 1.2 billion fine; confirmed that corporate surveillance at scale cannot be legitimised through consent engineering |

### A. K.S. Puttaswamy v. Union of India (2017): India's Constitutional Watershed

The Puttaswamy judgment is the most consequential Indian judicial pronouncement on privacy in a generation. The case arose from a challenge to the constitutional validity of the Aadhaar biometric identification scheme, but the nine-judge bench chose to resolve a prior question: whether the Constitution guarantees any right to privacy at all.

The court held, unanimously, that it does. Privacy was located within the right to life and personal liberty under Article 21 and was also found to be implicit in the freedoms of Articles 14 and 19. Crucially, the bench specified that any infringement of the right to privacy must satisfy a three-part test: it must be sanctioned by law; it must pursue a legitimate state aim; and it must be proportionate to that aim.[15] This proportionality framework provides the constitutional vocabulary for evaluating surveillance capitalism's encroachments. A private entity that harvests user data beyond what is necessary for a stated purpose, and repurposes that data for commercial manipulation, would struggle to satisfy the proportionality standard.

### B. Google Spain v. AEPD (2014): The Right to Be Forgotten

The CJEU's landmark ruling in Google Spain established that search engines are 'controllers' of the personal data they index and display, and that individuals have a qualified right to request the removal of links to information about them that is no longer relevant, excessive, or accurate.[16] The decision was significant not only for its substantive recognition of the 'right to be forgotten' but for its jurisdictional logic: EU data protection law applied wherever a European resident's data was processed, regardless of where the processing enterprise was headquartered.

The Google Spain ruling signalled a broader principle: that the commercial activity of a data-processing enterprise does not override the fundamental rights of the individuals whose data is processed. This principle would be carried forward and radically extended in the Schrems litigation.

[15]Nidhi Singh, Defining the Right to Privacy in India in Light of Justice KS Puttaswamy v. Union of India (2017), OXFORD HUM. RTS. HUB (Oct. 5, 2017), https://ohrh.law.ox.ac.uk.
[16]*Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, [2014] 3 C.M.L.R. 50 (Grand Chamber).

### C. Schrems II (2020): Surveillance States and Transatlantic Data Flows

The Schrems II decision of July 2020 arose from Austrian privacy activist Maximilian Schrems' challenge to the transfer of his Facebook data from the European Union to the United States.[17] His core contention was that US surveillance law, particularly Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, permitted US intelligence agencies to access EU residents' data without meaningful judicial oversight or remedy, in violation of their fundamental rights under the EU Charter.

The CJEU agreed, and struck down the EU-US Privacy Shield framework as inadequate. The court found that US surveillance programmes were not limited to what is strictly necessary and proportionate, as required by Article 52 of the EU Charter, and that EU data subjects lacked effective judicial redress in the United States.[18] The Meta Platforms fine of EUR 1.2 billion imposed by the Irish Data Protection Commission in May 2023 was the direct successor to Schrems II: it was issued precisely because Meta continued to transfer EU user data to the US on the basis of Standard Contractual Clauses that could not compensate for the structural inadequacy of US surveillance law.[19]

### D. Carpenter v. United States (2018): Digital Location Data and the Fourth Amendment

In the United States, the Supreme Court's decision in Carpenter v. United States represented a significant departure from decades of jurisprudence governed by the third-party doctrine.[20] Under that doctrine, established in cases such as Smith v. Maryland (1979),[21] information voluntarily disclosed to a third party carries no Fourth Amendment protection, because the individual has assumed the risk that the third party might share the information with the government.

Chief Justice Roberts, writing for a 5-4 majority, held that this doctrine, developed in an era of limited data disclosure, could not be mechanically applied to digital cell-site location information (CSLI). Mapping an individual's phone location across 127 days, the Chief Justice

[17] *Data Protection Commissioner v. Facebook Ireland Ltd. & Maximilian Schrems* (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (C.J.E.U. 2020).
[18] *Schrems II*, Case C-311/18, ¶ 179.
[19] European Data Prot. Bd., 1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision (May 22, 2023), https://www.edpb.europa.eu.
[20] *Carpenter v. United States*, 585 U.S. 296 (2018).
[21] Smith v. Maryland, 442 U.S. 735 (1979).

wrote, provides 'an all-encompassing record of the holder's whereabouts' akin to 'near perfect surveillance,' and a warrant was therefore required.[22] The decision stopped short of overruling the third-party doctrine but acknowledged its limitations in the digital context, leaving open questions that courts continue to navigate.

## V. REGULATORY RESPONSES: A COMPARATIVE EVALUATION

The following tables offer a comparative overview of the primary regulatory frameworks governing data protection and their enforcement record.

***Table 2: Comparative Regulatory Frameworks Across Jurisdictions***

| Jurisdiction | Primary Law | Privacy Right | Regulator | Max Penalty |
|---|---|---|---|---|
| European Union | GDPR (2016/679) | Arts. 7 & 8 EU Charter | National DPAs / EDPB | 4% global turnover |
| India | DPDPA 2023 | Art. 21, Constitution | Data Protection Board | INR 250 crore |
| United States | Sectoral (FTC, CCPA) | Fourth Amendment | FTC / State AGs | Variable / State-level |
| United Kingdom | UK GDPR / DPA 2018 | HRA 1998 (Art. 8 ECHR) | ICO | £17.5M or 4% turnover |
| Brazil | LGPD (2018) | Constitutional Art. 5 | ANPD | 2% national revenue |

### A. The GDPR: Europe's Rights-Based Paradigm

The General Data Protection Regulation, which entered into force in May 2018, is the most comprehensive data protection instrument in the world and the clearest legislative expression of the proposition that data protection is a fundamental right, not merely a regulatory preference. Its architecture is built around seven principles: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.[23]

[22]Carpenter v. United States, 585 U.S. at 315.
[23]GDPR arts. 5(1)(a), 5(1)(b).

For surveillance capitalism specifically, the most significant provisions are those governing consent and legitimate interest. The GDPR requires that consent be freely given, specific, informed, and unambiguous. The practice of making service access conditional on consent to behavioural advertising fails this standard, as the EUR 390 million fine imposed on Meta in January 2023 for exactly this practice confirms.[24]

GDPR enforcement has escalated dramatically. In 2023 alone, approximately EUR 2.1 billion in fines were imposed across the EU, driven primarily by the Meta transfer fine. As the chart below illustrates, average fines per violation have increased almost tenfold since 2019.

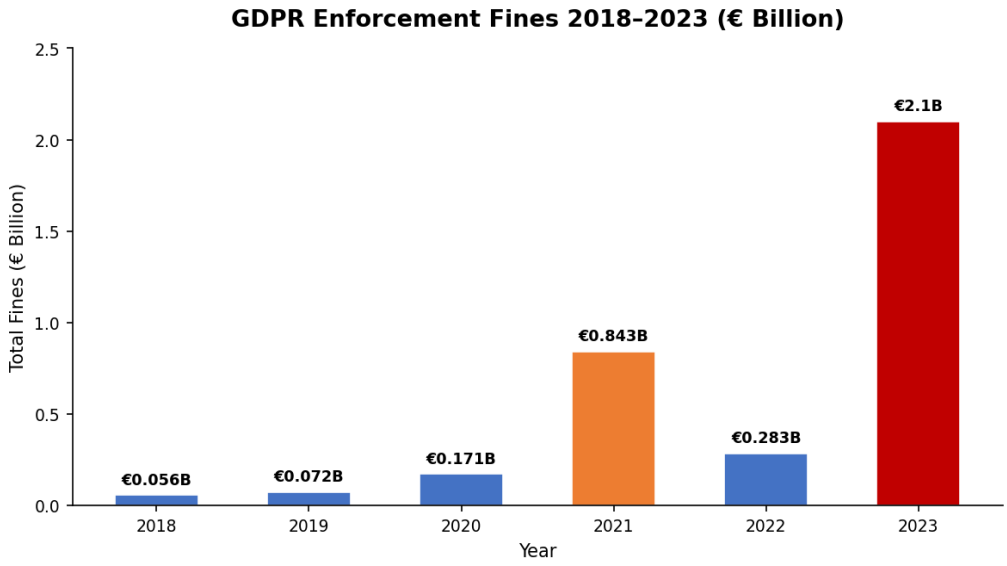



*Figure 2: Total GDPR Enforcement Fines by Year, 2018-2023 (EUR Billion). Source: Enforcement Tracker / Statista.*

**B. India's Digital Personal Data Protection Act, 2023**

India's Digital Personal Data Protection Act, 2023 (DPDPA), is the country's first comprehensive data protection legislation, enacted in August 2023 and progressively operationalised through the DPDP Rules, 2025.[25] It represents a significant advance over the patchwork of IT Act provisions and sector-specific rules that previously governed data protection in India.

The DPDPA requires explicit, purpose-specific consent for data processing and grants data

[24] *Id.* art. 83(5).
[25] Digital Personal Data Protection Act, No. 22 of 2023, § 4 (India).

principal rights of access, correction, erasure, and grievance redressal.[26] Significant data fiduciaries, those platforms and entities designated by the government as posing heightened risks to privacy, are subject to additional obligations including the appointment of Data Protection Officers, data protection impact assessments, and independent audits.

The penalties prescribed under the DPDPA are substantial for Indian conditions, reaching INR 250 crore (approximately USD 30 million) for the most serious breaches.[27] However, the regime has attracted criticism on two fronts. First, the government exemptions under Section 17 are wider than their GDPR counterparts and lack explicit proportionality requirements, raising concerns that state surveillance activity may escape accountability. Second, the independence of the Data Protection Board, whose members are government-appointed, has been questioned by civil society organisations.

A detailed comparison of the GDPR and DPDPA frameworks is set out below.

***Table 3: GDPR (EU) vs. DPDPA 2023 (India) -- A Comparative Analysis***

| Parameter | GDPR (EU) | DPDPA 2023 (India) |
|---|---|---|
| Territorial Scope | Applies wherever EU residents' data is processed | Applies to processing within India and processing targeting Indian residents abroad |
| Consent Standard | Freely given, specific, informed, unambiguous | Explicit consent; purpose-specific; withdrawal permitted |
| Data Subject Rights | Access, rectification, erasure, portability, objection | Access, correction, erasure, grievance redressal; no explicit portability right |
| Children's Data | Special protections; parental consent below 16 (varies by state) | Verifiable consent required; processing to harm children prohibited |
| Max Penalty | EUR 20M or 4% global annual turnover | INR 250 crore (approx. USD 30 million) |

[26] *Id.* § 5.
[27] *Id.* §§ 40–45.

| | | |
|---|---|---|
| Government Exemptions | Narrow; subject to proportionality review | Broader; state surveillance exemptions subject to criticism |
| Independent Regulator | Fully independent National DPAs | Data Protection Board -- independence concerns raised |

### C. The United States: Sectoral Fragmentation and the Limits of Self-Regulation

The United States lacks a federal omnibus data protection law. Privacy is governed by a patchwork of sectoral statutes: the Health Insurance Portability and Accountability Act for medical data, the Children's Online Privacy Protection Act for minors' data, the Gramm-Leach-Bliley Act for financial data, and the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), at the state level.[28]

The Federal Trade Commission exercises a general jurisdiction over unfair or deceptive trade practices that encompasses some data privacy violations, but its enforcement powers are reactive rather than prescriptive: it cannot impose ex ante rules with the clarity of the GDPR. The result is a regulatory environment that is broadly permissive toward surveillance capitalism, a consequence that reflects both the historical strength of American industry lobbying and a genuine constitutional scepticism, in some quarters, of proactive government regulation of commerce.

### D. The EU AI Act: Anticipating Tomorrow's Surveillance Instruments

The Regulation (EU) 2024/1689, known as the AI Act, entered into force on 1 August 2024 and represents the world's first comprehensive legal framework specifically governing artificial intelligence.[29] Its relevance to surveillance capitalism is direct: many of the most invasive data-processing practices of the modern economy, real-time biometric identification, emotion detection, behavioural scoring, and targeted manipulation, fall within the Act's ambit.

The AI Act classifies AI systems by risk level. Systems that deploy subliminal techniques to manipulate behaviour, exploit vulnerabilities of specific groups, and conduct real-time remote biometric identification in public spaces are, subject to narrow exceptions, prohibited.[30] High-

[28]Paul M. Schwartz & Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, 106 GEO. L.J. 115, 118 (2017).
[29]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).
[30]Artificial Intelligence Act art. 5(1)(c), Regulation (EU) 2024/1689.

risk AI systems, which include biometric identification, critical infrastructure management, and AI systems affecting access to education, employment, and essential services, must undergo conformity assessment before deployment.

The Act does not resolve all tensions between AI-driven surveillance and fundamental rights, but it represents a significant conceptual step: it treats the manipulation of human behaviour through AI as a matter of regulatory concern, not merely a question of consumer preference.

## VI. IDENTIFYING THE LACUNAE

The regulatory landscape surveyed above, though considerably more developed than it was a decade ago, contains several significant gaps that surveillance capitalism continues to exploit.

### A. The Commodification of Consent

Consent, as currently structured in most legal frameworks, is insufficient to the task of regulating surveillance capitalism. The GDPR requires that consent be 'freely given,' but consent cannot be freely given when the alternative to consenting is exclusion from digital services that have become, in practical terms, essential infrastructure.[31] Social media platforms, navigation services, and cloud-based productivity tools are not genuine luxuries from which users can readily walk away. The 'take it or leave it' character of digital service contracts renders the consent offered within them fundamentally coerced.

The deeper problem is informational asymmetry. A user who ticks a consent box on a privacy policy does not know, and cannot reasonably be expected to know, the full scope of downstream data processing: the third-party data brokers to whom profiles may be sold, the insurance companies that may access them, or the political consultancies that might use them. Consent to data processing is, in this sense, structurally unlike consent to other legal transactions. The object of the consent is too complex, too opaque, and too consequential for the model of individual rational consent to bear the weight placed on it.

### B. Enforcement Deficits and Structural Capture

Even where robust legal standards exist, enforcement is frequently inadequate. The Irish Data

[31]GDPR pmbl. recital 4.

Protection Commission, which is the lead European regulator for most of the major US technology platforms by virtue of their EU headquarters being located in Ireland, faced sustained criticism for the slow pace of its GDPR investigations.[32] The Meta transfer fine was the product of a 2020 complaint that took three years to resolve, and required intervention by the European Data Protection Board to overcome the Irish regulator's initial reluctance to impose a fine at all.

This is not merely an Irish problem. Data protection authorities across the EU operate with budgets that are a fraction of the compliance departments of the companies they regulate. The structural mismatch between regulatory capacity and corporate resources is a systemic feature of the current framework, not a correctable individual failure.

### C. Global Regulatory Fragmentation

Data does not stop at borders, but regulation does. Approximately 78 of the world's 197 countries have enacted comprehensive data protection frameworks; a further 54 have partial frameworks; 38 have only sector-specific rules; and 27 have no meaningful framework at all.[33] The chart below illustrates this distribution.

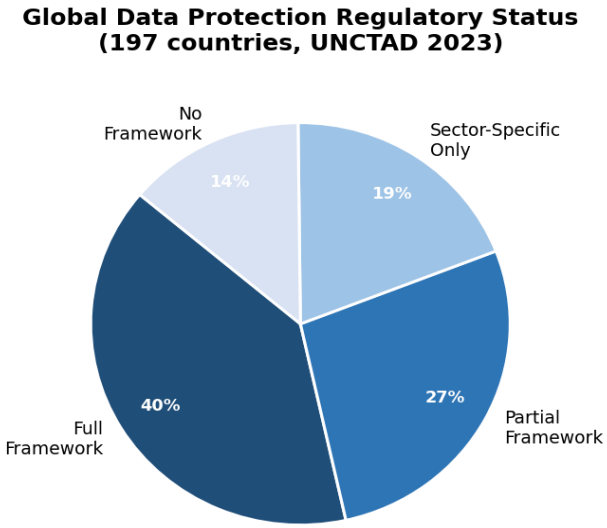



*Figure 3: Global Data Protection Regulatory Status (197 Countries). Source: UNCTAD, 2023.*

[32]Statista, GDPR Data Protection Fines Timeline, https://www.statista.com (last visited June 5, 2026).
[33]U.N. Conf. on Trade & Dev. (UNCTAD), Data Protection and Privacy Legislation Worldwide, https://unctad.org (last visited June 5, 2026).

This fragmentation creates a structural incentive for 'regulatory arbitrage': companies can route data processing through jurisdictions with weaker protections to escape the obligations imposed by stricter regimes. The adequacy decision mechanism under the GDPR, which permits data transfers to third countries only if they offer equivalent protection, is the primary instrument for addressing this problem, but it is slow, politically contested, and does not cover many of the world's largest economies.

### D. The Accountability Gap in Algorithmic Decision-Making

Perhaps the most profound lacuna in current frameworks is the absence of meaningful accountability for algorithmic decision-making that uses behavioural data to make or inform consequential decisions about individuals.[34] Credit scoring, insurance pricing, employment screening, and even criminal justice risk assessments increasingly rely on profiles assembled through surveillance capitalism's data infrastructure. The individuals affected by these decisions typically have no access to the data used, no understanding of the algorithm applied, and no effective means of challenging the outcome.

The GDPR's Article 22 provides a right not to be subject to solely automated decision-making that produces significant effects, and a right to request human review. But the provision is narrowly interpreted and rarely enforced in practice. The DPDPA 2023 does not contain an equivalent provision. And outside Europe, there is no general legal instrument that addresses this accountability gap.

## VII. TOWARDS A RIGHTS-ANCHORED REGULATORY MODEL: CONSTRUCTIVE PROPOSALS

The foregoing analysis suggests that incremental reform within existing frameworks is necessary but insufficient. What is needed is a more fundamental rethinking of the relationship between the data economy and fundamental rights. The following proposals are offered in that spirit.

### A. Structural Prohibition of Predatory Data Practices

Certain data practices are so intrinsically incompatible with fundamental rights that they should

[34]BRUCE SCHNEIER, *CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD* 34 (W.W. Norton & Co. 2018).

be prohibited outright rather than subjected to consent management. The use of intimate data to construct psychological profiles for political micro-targeting, the sale of health and location data to insurance companies without individual knowledge, and the deployment of real-time biometric identification for commercial purposes should be treated as per se unlawful under any serious rights-based framework.[35] The EU AI Act's prohibition on AI systems that exploit psychological vulnerabilities points in this direction; the concept should be extended and made more precisely applicable to the data-collection layer that precedes any particular AI application.

### B. Reconceptualising Consent as a Collective, Structural Matter

Given the structural inadequacy of individualised consent as a mechanism for regulating surveillance capitalism, regulatory frameworks should increasingly treat data protection as a collective and structural concern rather than as a matter of individual contractual choice. This means, practically, that data protection authorities should have the power to examine and prohibit entire categories of data practice, regardless of whether individual consent has technically been obtained.[36] It also means taking seriously the European concept of 'data minimisation': the obligation not merely to obtain consent for data collection but to collect only the data that is strictly necessary for a specified purpose.

### C. Strengthening Regulatory Capacity and Independence

Effective enforcement requires regulators that are adequately resourced, genuinely independent, and equipped with powers commensurate with the scale of the entities they regulate. The Indian DPDPA's Data Protection Board should be restructured to ensure genuine independence from government, as the Puttaswamy court's proportionality framework demands.[37] EU member states should substantially increase the budgets of national data protection authorities. And consideration should be given, at the international level, to a mechanism for mutual recognition and coordination of data protection enforcement, analogous to the instruments that exist in competition law.

---

[35]MARK COECKELBERGH, *AI ETHICS* 112 (MIT Press 2020).

[36]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM (2020) 66 final (Feb. 19, 2020).

[37]Rohan Grover, India's Digital Personal Data Protection Act 2023: A Critical Analysis, 9 INDIAN J. L. & TECH. 44, 49 (2024).

### D. A Right to Data Sovereignty

Current frameworks grant individuals rights in relation to their data: access, rectification, erasure. These rights are important but reactive. A more ambitious approach would recognise data sovereignty as a proactive right: the right of individuals to determine, not merely to respond to, the conditions under which their data is collected and processed. This would imply, at minimum, a right to data portability that is technically meaningful (enabling individuals to move their data between platforms), a right to algorithmically generated explanations of consequential decisions, and a right to opt out of surveillance-based advertising as a default, not a difficult-to-find setting.

### E. International Harmonisation Towards a Minimum Rights Floor

Regulatory arbitrage can only be effectively addressed through international cooperation. The existing framework of bilateral adequacy decisions is inadequate to the scale of the problem. Consideration should be given to a multilateral convention on data protection and digital rights, building on the Council of Europe's Convention 108+, that establishes a minimum floor of protection applicable in all participating states and provides a mechanism for addressing non-compliance by major data-processing companies regardless of where they are incorporated.

## VIII. CONCLUSION

Surveillance capitalism is not a temporary feature of the digital economy that can be corrected by better consent forms or higher fines. It is, as Zuboff argues, a new economic logic: an attempt to make the accumulation of knowledge about human behaviour the primary axis of economic value. That logic is, by its nature, in tension with the foundations of a rights-based liberal order.

The courts in Puttaswamy, Google Spain, Schrems II, and Carpenter have each recognised, in different registers and to different degrees, that the rights of the individual cannot simply be dissolved in the acid of commercial convenience. The legislatures of the European Union and India have attempted, with partial success, to translate that judicial recognition into operational legal frameworks. And the EU AI Act represents the first serious attempt to address the next generation of surveillance tools before they become entrenched.

But significant gaps remain. Consent is structurally inadequate as the primary regulatory

mechanism. Enforcement is unevenly resourced and insufficiently aggressive. Regulatory fragmentation permits global companies to arbitrage the differences between jurisdictions. And the accountability gap in algorithmic decision-making remains largely unaddressed by existing law.

What is ultimately at stake is not merely the privacy of individual users. It is the epistemic and political infrastructure of democratic societies. When the information environment is shaped by commercial algorithms designed to maximise engagement rather than to inform, and when political campaigns can use surveillance capitalism's data infrastructure to identify and psychologically manipulate voters with surgical precision, the foundations of democratic deliberation are themselves at risk.

A rights-anchored regulatory model, one that treats data sovereignty as a precondition of democratic freedom rather than as a consumer preference, is not a luxury for wealthy jurisdictions. It is a necessity for any political community that takes seriously the commitments expressed in its constitutional instruments. The challenge for legal scholars, regulators, and legislators in the years ahead is to build that model before surveillance capitalism's encroachments become irreversible.