International Journal of Economic Practices and Theories (IJEPT)
ISSN: 2247-7225
Volume 2026, Issue 1

Surveillance Pricing and Consumer Autonomy: Regulating AI-Driven Algorithmic Price Discrimination in Digital Marketplaces across the United States, the European Union, and India

Sneha

Assistant Professor of Law, Xavier Law School, XIM University, Bhubaneswar

ABSTRACT

The proliferation of artificial intelligence in digital marketplaces has enabled a commercial practice that regulatory authorities now term surveillance pricing. Online retailers and digital platforms deploy AI-driven algorithms that analyse consumer data including browsing history, geographic location, purchase patterns, and demographic profiles to generate individualised prices for identical goods and services. Preliminary findings from a federal market study in the United States released in January 2025 confirmed the widespread extraction of granular personal data for price personalisation. Legislative responses have since proliferated across multiple jurisdictions. New York enacted the first state-level algorithmic pricing disclosure law, effective November 2025. Maryland signed legislation restricting AI-enabled pricing in food retail in April 2026. The first comprehensive state-level AI governance statute targeting high-risk systems takes effect in Colorado in June 2026. More than forty state-level bills across twenty-four states were introduced in the first quarter of 2026 alone. The European Union addresses algorithmic pricing through overlapping instruments, principally its AI Act, data protection regulation, and digital services legislation. India has responded through consumer protection statutes, dark patterns guidelines, data protection legislation, and implementing rules that impose algorithmic due diligence obligations on significant data fiduciaries. Doctrinal and comparative legal research methods structure the analysis across these three jurisdictions. Findings reveal a regulatory spectrum from transparency-focused disclosure mandates in the United States to comprehensive risk-based governance in the European Union to an evolving sectoral approach in India. Consumer pricing transparency emerges as a component of algorithmic fairness. A model regulatory framework combining mandatory disclosure, algorithmic auditing, and sector-specific prohibitions on discriminatory pricing practices is proposed.

Keywords: *surveillance pricing, algorithmic price discrimination, consumer protection, AI regulation, digital human rights, comparative law*

INTRODUCTION

Artificial intelligence has transformed the commercial relationship between digital platforms and consumers. Algorithmic systems now observe, record, and analyse consumer behaviour at a granular level to determine the prices that individual buyers encounter for identical products. The Federal Trade Commission of the United States coined the term surveillance pricing to describe this practice, defining it as the deployment of advanced data collection technologies to adjust prices based on competitor pricing, precise location, browser history, purchase history, consumer preferences, and demographics (Federal Trade Commission, 2025). The phenomenon is not new in economic theory. Price discrimination has existed across multiple degrees since classical economic taxonomy. What distinguishes surveillance pricing from its antecedents is the scale, precision, and opacity of the underlying algorithmic infrastructure.

Digital platforms accumulate vast datasets from consumer interactions. Every click, search query, device identifier, and geolocation signal feeds into machine learning models that predict individual willingness to pay. A consumer searching for baby products while exhibiting browsing patterns consistent with new parenthood may encounter different prices than a consumer with a different behavioural profile, even for the same item at the same moment (Federal Trade Commission, 2025). The asymmetry between the platform's informational advantage and the

consumer's ignorance of the pricing mechanism raises fundamental concerns about fairness, autonomy, and the integrity of digital marketplaces.

Regulatory attention intensified in 2024 when the Federal Trade Commission initiated a Section 6(b) market study into surveillance pricing practices. By January 2025, preliminary findings confirmed that companies routinely leveraged highly sensitive personal data to calibrate individualised prices (Federal Trade Commission, 2025). The political response was swift and geographically dispersed. State legislatures across the United States introduced more than forty bills targeting algorithmic pricing in the first quarter of 2026 alone, surpassing the total number introduced throughout 2025 (Inside Privacy, 2026). The European Union addressed the phenomenon through a layered regulatory architecture combining its AI Act, the General Data Protection Regulation, and the Digital Services Act. India responded through a combination of consumer protection statutes, data protection legislation, and dark patterns guidelines, though without a dedicated instrument targeting surveillance pricing as a discrete consumer harm. The rapid proliferation of regulatory responses across these three jurisdictions, each representing a distinct governance model and legal tradition, creates the conditions for meaningful comparative analysis.

The research objective is to conduct a comparative legal analysis of regulatory responses to AI-driven surveillance pricing across the United States, the European Union, and India. The analysis assesses whether existing frameworks adequately protect consumer autonomy in algorithmic marketplaces.

LITERATURE REVIEW

Scholarship on algorithmic pricing has evolved significantly since the mid-2010s, when academic attention first turned to the consumer welfare implications of personalised pricing in digital markets. Algorithmic price discrimination generates measurable psychological harm among consumers. Experimental research involving 696 participants across two studies found that increased price discrimination leads to heightened perceptions of betrayal and diminished perceptions of price fairness (Wu et al., 2022). Perceived ease of use of online retail platforms moderates that relationship, suggesting that consumer familiarity with a platform does not eliminate the harm but rather tempers its intensity. The integration of discrimination and fairness as analytical constructs has since become a central feature of algorithmic pricing scholarship.

The intersection of artificial intelligence, firm behaviour, and consumer welfare has generated a distinct strand of survey literature. AI systems enable firms to extract consumer surplus with unprecedented precision, raising questions about the distribution of welfare gains between platforms and their users (Abrardi et al., 2021). A significant gap exists between the technical capabilities of algorithmic pricing systems and the capacity of existing regulatory frameworks to govern them. That gap has widened as pricing algorithms have become more sophisticated and data collection practices more pervasive.

The concept of surveillance pricing as a regulatory category gained traction following the Federal Trade Commission's 2024 initiation of its Section 6(b) study. The FTC framed surveillance pricing as distinct from conventional dynamic pricing, which responds to supply and demand fluctuations, by emphasising the personalised and data-intensive character of the practice (Federal Trade Commission, 2025). A comparative analysis of personalised algorithmic pricing and consumer protection across the United States, the European Union, and India found that regulatory coherence remains limited, with fragmented enforcement mechanisms undermining the effectiveness of consumer protection across all three jurisdictions (Mone et al., 2026). The persistence of this fragmentation despite legislative momentum in each jurisdiction suggests that the problem is structural rather than merely temporal.

The relationship between algorithmic pricing and consumer autonomy has attracted attention from digital rights scholars. Consumer autonomy in this context refers to the capacity of individuals to make purchasing decisions based on accurate, transparent, and non-manipulated information. Existing consumer protection frameworks require adaptation to address the specific harms generated by algorithmic pricing, and pricing transparency constitutes a

necessary condition for meaningful consumer choice in algorithmically mediated marketplaces (Frazier, 2025). That argument reframes the regulatory question from one of market efficiency to one of rights. If consumers cannot access accurate pricing information because the pricing mechanism is opaque by design, the conditions for autonomous consumer choice are absent.

Scholarship on dark patterns has also contributed to the understanding of algorithmic consumer manipulation. Dark patterns, as originally defined by user experience designer Harry Brignull, are deceptive interface designs that trick users into making choices against their interests. The concept has expanded to encompass algorithmic pricing practices such as drip pricing, where additional charges are incrementally disclosed during a transaction (Central Consumer Protection Authority, 2023). The International Association of Privacy Professionals noted in February 2026 that India's regulatory response to dark patterns remains soft, lacking the enforcement infrastructure to translate guidelines into effective consumer protection (IAPP, 2026).

The ethics of personalised pricing have generated a parallel strand of scholarly debate. Traditional economic analysis treats price discrimination as welfare-enhancing when it expands market access by allowing lower prices for price-sensitive consumers. The surveillance pricing context complicates this analysis. The welfare-enhancing rationale depends on a competitive market structure in which consumers can substitute between providers. Dominant digital platforms operating in winner-take-most market structures limit substitution possibilities, converting personalised pricing from a welfare-enhancing mechanism into a surplus-extraction tool. Start-ups and scale-ups deploying algorithmic pricing systems face particular reputational and legitimacy risks when consumer trust in algorithmic fairness erodes, and the intersection between algorithmic design, normative imperatives, and consumer-centric outcomes remains conceptually fragmented (de Lucas López et al., 2026).

India's regulatory trajectory has drawn specific scholarly attention. India entered its largest digital consumer marketplace phase without a dedicated legal framework for algorithmic consumer protection (Policy Circle, 2026). The country had more than one billion internet subscribers at the end of December 2025, and its e-commerce market is projected to reach approximately 345 billion dollars by 2030. Indian law addresses data collection with greater clarity than it addresses the use of algorithms to shape consumer choice in real time. That asymmetry constitutes the central policy gap. India does not need to replicate the European privacy regime or the Chinese platform control model. It requires a framework built on enforceable consumer protection principles shaped by domestic conceptions of fairness (Policy Circle, 2026).

A research gap persists in the comparative legal literature. Existing tri-jurisdictional studies tend to address AI governance broadly without isolating surveillance pricing as a discrete regulatory problem. The rapid legislative developments across the United States, the European Union, and India in 2025 and 2026 have outpaced academic analysis. Scholarship has not yet systematically compared the transparency-versus-prohibition spectrum that characterises emerging regulatory responses. Nor has it assessed the specific adequacy of India's evolving framework against the more advanced instruments deployed in the other two jurisdictions.

METHODOLOGY

The research adopts a doctrinal and comparative legal methodology. Doctrinal analysis examines the text, structure, and interpretive context of primary legal instruments governing surveillance pricing across the three selected jurisdictions. Primary sources include statutes, regulations, regulatory reports, and official legislative records. Secondary sources include peer-reviewed scholarship, policy analyses published by law firms and research institutions, and reports from international organisations.

The selection of the United States, the European Union, and India as comparators follows a most-different-systems design. The United States represents a decentralised, state-driven regulatory model with overlapping federal enforcement. The European Union represents a comprehensive, supranational, risk-based governance framework. India represents an emerging regulatory jurisdiction combining sectoral consumer protection instruments with newly

enacted data protection legislation. The three jurisdictions collectively account for a substantial share of global digital commerce and represent distinct legal traditions, governance structures, and stages of regulatory maturity in AI governance.

The temporal scope of the analysis extends from the Federal Trade Commission's initiation of its Section 6(b) study in July 2024 through May 2026. This period captures the most significant legislative and regulatory developments across all three jurisdictions. The analytical framework is structured around three dimensions of comparison, being transparency and disclosure requirements, algorithmic auditing and accountability obligations, and substantive prohibitions on discriminatory pricing practices. Comparative findings are synthesised in the Discussion section, where their implications for consumer autonomy are assessed.

RESULTS

The United States: Fragmented State Innovation and Federal Scrutiny

The regulatory response to surveillance pricing in the United States is characterised by simultaneous federal investigation and decentralised state legislation, with developments accelerating sharply between 2024 and 2026 (see Table 1). The Federal Trade Commission initiated its Section 6(b) market study in July 2024, ordering eight intermediary firms to disclose their development and deployment of surveillance pricing products (Federal Trade Commission, 2025). The firms ordered to produce information included Mastercard, JPMorgan Chase, Accenture, McKinsey, Revionics, Bloomreach, PROS, and Task Software. The January 2025 preliminary findings revealed that these firms utilised a wide range of personal data, from precise geolocation and demographics to mouse movements and browsing patterns, to generate individualised pricing recommendations for retailers (Federal Trade Commission, 2025). The FTC approved the release of the study in a three-to-two vote along party lines, with Republican commissioners issuing a dissenting statement.

Table 1. Timeline of Key Legislative and Regulatory Developments in Surveillance Pricing Governance (2023–2026)

Date	Jurisdiction	Development
November 2023	India	CCPA issues Guidelines for Prevention and Regulation of Dark Patterns under Section 18, CPA 2019, identifying 13 specified patterns
May 2024	United States	Colorado enacts Consumer Protections for Artificial Intelligence Act (SB 24-205); effective date later delayed to 30 June 2026
June 2024	European Union	EU AI Act adopted (Regulation (EU) 2024/1689) with risk-based classification framework
July 2024	United States / EU	FTC initiates Section 6(b) surveillance pricing study ordering 8 intermediary firms to disclose practices; EU Commission launches AI-in-contracting workstream
January 2025	United States	FTC releases preliminary findings confirming widespread use of personal data for individualised pricing (3-2 party-line vote)
August 2025	European Union	EU AI Act general-purpose AI model provisions become applicable (full enforcement powers from August 2026)

November 2025	United States	New York Algorithmic Pricing Disclosure Act takes effect; first state-level surveillance pricing disclosure law
November 2025	India	DPDP Rules 2025 notified (13 November); Data Protection Board established; algorithmic due diligence obligation for SDFs introduced under Rule 13
December 2025	India / US	AI (Ethics and Accountability) Bill 2025 introduced in Lok Sabha; White House issues Executive Order citing excessive state AI regulation
Q1 2026	United States	40+ algorithmic pricing bills introduced across 24 states; House Oversight Committee launches investigation (5 March 2026)
April 2026	United States	Maryland signs Protection From Predatory Pricing Act (HB 895); restricts AI-enabled pricing in food retail; effective 1 October 2026
June 2026	United States	Colorado Consumer Protections for AI Act takes effect; first comprehensive US state AI governance statute

New York enacted the first state-level surveillance pricing disclosure law in the nation. The Algorithmic Pricing Disclosure Act, signed by Governor Kathy Hochul and effective since November 2025, requires businesses that use algorithms to set prices based on personal consumer data to display a conspicuous disclosure. The required text states in all capitals that the price was set by an algorithm using personal data (Skadden, Arps, Slate, Meagher & Flom LLP, 2026). Attorney General Letitia James issued a consumer alert encouraging consumers to report non-compliant businesses. Civil penalties of up to one thousand dollars per violation apply. The law exempts loyalty programmes, coupons, and temporary promotional pricing. A legal challenge brought by the National Retail Federation remains pending, and the Attorney General paused enforcement during the preliminary injunction proceedings in July 2025.

Maryland adopted a more restrictive approach than New York. Governor Wes Moore signed the Protection From Predatory Pricing Act (House Bill 895) on 28 April 2026, effective 1 October 2026. The Act restricts personalised pricing, consumer data-driven pricing, and AI-enabled pricing practices in food retail establishments exceeding fifteen thousand square feet and in third-party food delivery platforms (Consumer Finance Monitor, 2026). The Maryland statute marks a departure from the disclosure-only model adopted by New York. It imposes substantive restrictions on the use of personal data in pricing decisions for essential consumer goods rather than simply requiring transparency.

The Colorado Consumer Protections for Artificial Intelligence Act (SB 24-205), enacted in May 2024 with an effective date delayed to 30 June 2026, represents the most comprehensive state-level AI governance statute in the United States. It requires developers and deployers of high-risk AI systems to exercise reasonable care to prevent algorithmic discrimination, conduct impact assessments, and provide consumer disclosures (Baker Botts LLP, 2026). Penalties of up to twenty thousand dollars per violation apply. No private right of action exists under the statute. The Act attracted explicit mention in the December 2025 White House Executive Order, which cited it as an example of what the federal government characterised as excessive state regulation impeding AI innovation.

Federal legislative proposals have proliferated alongside state action. The Stop AI Price Gouging and Wage Fixing Act of 2025 and the One Fair Price Act of 2025 seek to prohibit surveillance-based pricing at the federal level

(WilmerHale, 2026). The AI Civil Rights Act, reintroduced in December 2025, proposes to bar discriminatory algorithmic practices and impose audit and notice requirements on firms deploying AI tools. On 5 March 2026, House Oversight Committee Chairman James Comer launched an investigation into the use of AI to analyse consumer data for price-setting, sending inquiry letters to travel accommodation and rideshare companies (WilmerHale, 2026). Attorney General offices in California, Utah, and North Carolina have also initiated collaborative enforcement actions targeting algorithmic pricing (American Bar Association, 2026).

The cumulative effect of these developments is a patchwork of regulatory obligations that vary significantly across states. Disclosure-only mandates in New York coexist with sector-specific prohibitions in Maryland and comprehensive AI governance requirements in Colorado. Federal legislation remains stalled despite broad bipartisan awareness of the issue. Forty bills across twenty-four states were introduced in the first quarter of 2026 alone, proposing approaches that ranged from general prohibitions to sector-specific restrictions to protected-class data bans in pricing decisions (Inside Privacy, 2026). Retailers and digital platforms operating nationally face substantial compliance complexity as a result.

The European Union: Layered Supranational Governance

The European Union addresses surveillance pricing through a layered regulatory architecture comprising the AI Act, the General Data Protection Regulation, and the Digital Services Act. No single instrument targets algorithmic pricing as a standalone regulatory concern. The governance framework relies on overlapping instruments that collectively constrain the deployment of AI-driven pricing systems.

The EU AI Act (Regulation (EU) 2024/1689) establishes a risk-based classification system for AI applications. Article 5(1)(c) prohibits AI systems that evaluate or classify individuals based on social behaviour or personal characteristics where such classification leads to detrimental or disproportionate treatment in unrelated contexts (Global Competition Review, 2025). AI systems used for credit scoring or insurance pricing fall within the Annex III high-risk category, requiring conformity assessments, risk management systems, and human oversight obligations. The general-purpose AI model provisions became applicable on 2 August 2025, with full enforcement powers including fines and model recalls activating on 2 August 2026. Algorithmic pricing systems deployed in e-commerce fall outside the explicit high-risk classifications but remain subject to general EU consumer protection and data protection law.

The General Data Protection Regulation provides a foundational constraint on surveillance pricing through Article 22. That provision grants individuals the right not to be subject to decisions based solely on automated processing that produce legal effects or similarly significant effects. Where an AI pricing algorithm generates an individualised price that materially affects a consumer's economic position, Article 22 arguably applies (Gunderson Dettmer, 2026). Data subjects retain the right to obtain human intervention, express their point of view, and contest the decision. The GDPR also mandates data protection impact assessments under Article 35 for processing operations involving systematic monitoring or automated decision-making with significant effects.

The Digital Services Act (Regulation (EU) 2022/2065) imposes transparency obligations on online platforms operating algorithmic recommender systems. While the DSA primarily addresses content moderation and platform accountability, its transparency requirements extend to algorithmic systems that influence the presentation of goods and services to consumers (Global Competition Review, 2025). Platforms must disclose the main parameters used in their recommender systems and provide consumers with options to modify those parameters. Where pricing recommendations form part of an algorithmic product display, the DSA's transparency provisions may require platforms to disclose the role of personal data in price determination.

The European Commission launched a dedicated workstream in July 2024 on AI in contracting, specifically examining scenarios in which machines make decisions without explicit human consent (Global Competition Review, 2025). This initiative signals a recognition that existing instruments may not fully address the specific consumer harms

generated by algorithmic pricing. The interplay between the AI Act's risk classifications, the GDPR's automated decision-making provisions, and the DSA's transparency obligations creates a dense regulatory environment. Firms operating within the EU must navigate multiple compliance regimes simultaneously. The regulatory density offers comprehensive coverage but also creates interpretive uncertainty about which instrument governs specific pricing practices.

India: Evolving Sectoral Responses and Regulatory Gaps

India's regulatory response to surveillance pricing is distributed across multiple statutes and instruments that were not originally designed to address AI-driven price personalisation. The Consumer Protection Act 2019 defines unfair trade practices under Section 2(47), encompassing deceptive methods such as misrepresenting product standards, falsely advertising old goods as new, and misrepresenting prices. The Act empowers the Central Consumer Protection Authority established under Section 10 to investigate consumer complaints, recall unsafe goods, and penalise misleading advertisements.

The CCPA issued the Guidelines for Prevention and Regulation of Dark Patterns on 30 November 2023 under Section 18 of the Consumer Protection Act 2019, identifying thirteen specified dark patterns (Press Information Bureau, 2023). The enumerated patterns include drip pricing, false urgency, basket sneaking, subscription traps, bait and switch, interface interference, confirm shaming, forced action, disguised advertisements, nagging, trick wording, SaaS billing, and rogue malware. The Guidelines apply to platforms offering goods or services in India, to advertisers, and to sellers. Drip pricing is the pattern most directly relevant to surveillance pricing, as it conceals the true cost of a product through staged disclosure of algorithmically determined charges. In early June 2025, the CCPA issued an advisory directing e-commerce platforms to conduct self-audits within three months to identify and eliminate dark patterns on their platforms (IAPP, 2026).

The Consumer Protection (E-Commerce) Rules 2020, notified under the Consumer Protection Act 2019, mandate that e-commerce entities integrate with the National Consumer Helpline, appoint grievance officers, and ensure transparent pricing. Draft amendments circulated in 2021 proposed a ban on flash sales that manipulate consumer choice and the introduction of fallback liability for platform defaults. These amendments remain unfinished, and the regulatory treatment of algorithmic pricing in e-commerce continues to be governed by the original 2020 Rules and the 2023 Dark Patterns Guidelines.

The Digital Personal Data Protection Act 2023 and the implementing DPDP Rules 2025, notified on 13 November 2025, introduce a consent-based data governance regime applicable to all data fiduciaries processing digital personal data in India (National Law Review, 2025). The Rules require Significant Data Fiduciaries to conduct annual data protection impact assessments and audits through independent data auditors (Lexology, 2025a). Rule 13 imposes an algorithmic due diligence obligation, requiring Significant Data Fiduciaries to verify that technical measures, including algorithmic software used to manage personal data, are not likely to pose a risk to the rights of data principals (S.S. Rana & Co., 2025). The SDF designation has not yet been applied to specific entities, and the main compliance obligations take effect in a phased manner, with the principal duties becoming operational by May 2027 (Lexology, 2025b). The gap between the statutory text and its enforcement therefore remains significant.

Amendments to the Consumer Protection Act introduced in 2025 expanded the scope of unfair trade practices to address dynamic pricing and algorithmic influence on consumer behaviour (SK Legal Consultancy, 2025). The amendments strengthened penalties for misleading advertisements and introduced provisions for faster dispute resolution within ninety days. They mandated that online marketplaces assume direct accountability for product authenticity and refunds. The amendments did not create a standalone prohibition on surveillance pricing or mandate consumer-facing algorithmic pricing disclosures equivalent to the New York model.

The Artificial Intelligence (Ethics and Accountability) Bill 2025, introduced as a Private Member's Bill in the Lok Sabha in December 2025, proposes a statutory Ethics Committee for AI, mandatory ethical reviews for

surveillance and high-risk AI systems, bias audits, developer obligations, restrictions on AI use in law enforcement and employment, grievance mechanisms, and penalties up to five crore rupees (TechPolicy.Press, 2026). The Bill has not been enacted and its prospects remain uncertain, though it signals growing parliamentary interest in binding AI accountability. The India AI Governance Guidelines released by MeitY in November 2025 under the IndiaAI Mission adopt a light-touch model emphasising innovation over regulation, and these guidelines lack the force of law.

The Competition Act 2002 offers an additional regulatory pathway through Section 4, which prohibits abuse of dominant position. Dark patterns deployed by market-dominant enterprises to manipulate consumer choice architecture could attract scrutiny under this provision (Legal 500, 2025). Algorithmic pricing that restricts consumer freedom of choice or denies competitors access to markets may constitute non-price exclusionary behaviour under Section 4. The Competition Commission of India has not yet pursued a case specifically targeting surveillance pricing, leaving this enforcement pathway untested.

DISCUSSION

The comparative analysis reveals three distinct regulatory models positioned along a spectrum from transparency to prohibition (see Table 2). The United States occupies the transparency-focused end at the state level, with New York's disclosure mandate representing the minimal regulatory intervention. Maryland's sector-specific restrictions on personalised pricing in essential goods mark a shift toward substantive prohibition. Colorado's comprehensive AI governance statute applies broadly to high-risk systems without targeting pricing as a discrete harm. The absence of enacted federal legislation creates a fragmented landscape in which compliance obligations vary by state, generating uncertainty for nationally operating digital platforms.

Table 2. Comparative Regulatory Framework for Surveillance Pricing across the United States, the European Union, and India

Regulatory Dimension	United States	European Union	India
Primary Instruments	State statutes (NY, MD, CO); FTC Section 6(b) study; pending federal bills	AI Act (2024); GDPR Article 22; Digital Services Act (2022)	CPA 2019; Dark Patterns Guidelines 2023; DPDP Act 2023 and Rules 2025; Competition Act 2002
Transparency and Disclosure	Mandatory consumer-facing disclosure (NY); conspicuous all-capitals notice when price set by algorithm using personal data	DSA requires disclosure of recommender system parameters; GDPR mandates information about automated decision-making	Dark Patterns Guidelines prohibit drip pricing; no mandatory algorithmic pricing disclosure equivalent to NY model
Algorithmic Auditing	Colorado AI Act requires impact assessments for high-risk AI systems; no federal audit mandate	GDPR Article 35 mandates DPIAs for systematic monitoring; AI Act requires conformity assessments for high-risk systems	DPDP Rules 2025 Rule 13 requires algorithmic due diligence for SDFs; annual DPIAs and independent audits
Substantive Prohibitions	Maryland restricts personalised pricing in food retail (15,000+ sq ft) and	AI Act Article 5(1)(c) prohibits detrimental social	CPA 2019 prohibits unfair trade practices; 2025 amendments address

	delivery; pending federal prohibition bills	scoring; no direct prohibition on personalised pricing	dynamic pricing; no standalone surveillance pricing prohibition
Enforcement Mechanism	State attorney general action; civil penalties up to USD 1,000 (NY) and USD 20,000 (CO) per violation; no private right of action (CO)	National supervisory authorities; AI Office enforcement from August 2026; fines under GDPR up to 4% of global turnover	CCPA enforcement; Data Protection Board (established November 2025); Competition Commission of India (untested for pricing)
Key Regulatory Gap	No federal legislation; fragmented state patchwork; compliance complexity for nationally operating platforms	No standalone surveillance pricing instrument; reliance on consumers to exercise GDPR Article 22 rights	SDF designation pending; weak CCPA enforcement capacity; no consumer-facing pricing disclosure mandate

The European Union occupies an intermediate position characterised by regulatory density rather than targeted intervention. The AI Act, the GDPR, and the DSA collectively constrain the conditions under which surveillance pricing can operate, but no single instrument prohibits the practice or mandates specific pricing disclosures. The strength of the EU model lies in its layered architecture, where data protection, algorithmic risk management, and platform transparency obligations converge to limit the informational asymmetry that enables surveillance pricing. The limitation of the EU model is its reliance on consumers to exercise their existing rights under Article 22 of the GDPR, which presupposes awareness that automated pricing decisions are occurring.

India occupies the most nascent position on the regulatory spectrum. The dark patterns framework, the DPDP Rules, and the 2025 amendments to the Consumer Protection Act collectively create the legal vocabulary necessary to address surveillance pricing, but they do not yet constitute a coherent regulatory regime. India lacks both a mandatory consumer-facing pricing disclosure equivalent to the New York model and sector-specific pricing restrictions equivalent to the Maryland statute. The algorithmic due diligence obligation under the DPDP Rules applies only to Significant Data Fiduciaries, a category that has not yet been operationalised through designation of specific entities. The CCPA's dark patterns enforcement capacity is limited by resource constraints, and the structural relationship between the Consumer Protection Act and the DPDP Act remains weak (IAPP, 2026).

A central finding of this analysis is that surveillance pricing operates at the intersection of three legal domains traditionally regulated separately. Consumer protection law addresses unfair trade practices, data protection law governs the collection and processing of personal data, and competition law addresses market power and exclusionary behaviour. Surveillance pricing exploits the gaps between these domains by generating harms that no single legal framework is designed to capture. A pricing algorithm that uses lawfully collected personal data to generate individualised prices may not violate data protection law if valid consent was obtained. It may not violate consumer protection law if the price itself is not deceptive. It may not violate competition law if the platform is not dominant. The harm to consumer autonomy arises from the interaction of these factors rather than from any single legal violation (Policy Circle, 2026).

The emergence of surveillance pricing as a regulatory concern supports the recognition of consumer pricing transparency as a component of the broader right to algorithmic fairness. Digital human rights scholarship has argued with increasing force that algorithmic systems mediating access to essential goods and services must be subject to transparency and accountability obligations. Pricing transparency in algorithmic marketplaces represents a logical

extension of this principle. Consumers cannot exercise meaningful choice if the prices they encounter are opaque products of data extraction processes they neither consented to nor understand. The New York disclosure requirement, despite its limitations, establishes a precedent for treating pricing transparency as a legal obligation rather than a voluntary practice.

Regulatory convergence across jurisdictions is unlikely in the near term given the structural differences in governance models. The United States is unlikely to adopt comprehensive federal legislation given the current executive emphasis on minimising regulatory burdens on AI innovation, as reflected in the December 2025 Executive Order. The European Union is unlikely to adopt a standalone surveillance pricing instrument given the density of its existing regulatory architecture. India occupies the most dynamic position on the regulatory landscape. The country has demonstrated the political will to regulate digital consumer harms through the dark patterns framework and the DPDP Act. What remains missing is the institutional capacity and regulatory specificity to translate that political will into effective surveillance pricing governance. India's stated ambition to lead global AI governance creates a domestic accountability standard that the current regulatory framework does not yet meet (Policy Circle, 2026).

The enforcement dimension presents distinct challenges across all three jurisdictions. The New York model depends on consumer awareness and willingness to report non-compliant businesses. A disclosure requirement is only as effective as the consumer's ability to interpret it and act on it. Consumers who are unaware of how personalised pricing operates are unlikely to recognise the significance of a disclosure, much less to report a violation. The Maryland model avoids this limitation by imposing outright restrictions on data-driven pricing in designated sectors, shifting the regulatory burden from the consumer to the firm. The Colorado model requires firms to conduct impact assessments and demonstrate reasonable care, but its enforcement mechanism relies on attorney general action rather than private claims. Each model addresses a different failure point in the regulatory chain.

The DPDP Rules' algorithmic due diligence requirement represents a promising instrument if it is operationalised effectively. The requirement that Significant Data Fiduciaries verify that algorithmic software does not pose risks to data principal rights could be interpreted to encompass surveillance pricing practices that extract consumer surplus through data exploitation (S.S. Rana & Co., 2025). The effectiveness of this provision depends on three factors. The first is the designation of entities as Significant Data Fiduciaries, which has not yet occurred. The second is the independence and technical competence of the data auditors who conduct the annual assessments. The third is the willingness of the Data Protection Board of India to enforce compliance findings with meaningful penalties. Without progress on all three fronts, the algorithmic due diligence obligation will remain a textual commitment without practical effect.

CONCLUSION

Surveillance pricing represents a consumer harm that existing legal frameworks across the United States, the European Union, and India address partially but not comprehensively. The United States has generated the most diverse regulatory responses, ranging from disclosure mandates to sector-specific prohibitions. The absence of federal legislation leaves consumer protection dependent on the legislative priorities of individual states. The European Union provides the most structurally coherent framework through the convergence of the AI Act, the GDPR, and the DSA. It lacks a targeted instrument addressing personalised pricing as a discrete consumer harm. India has built the necessary legislative vocabulary through the Consumer Protection Act 2019, the Dark Patterns Guidelines, the DPDP Act, and the 2025 amendments. Enforcement capacity and regulatory specificity remain underdeveloped.

A model regulatory framework for surveillance pricing governance would combine three elements. The first is mandatory consumer-facing disclosure modelled on the New York approach, requiring platforms to inform consumers when prices are generated by algorithms using personal data. The second is algorithmic auditing obligations modelled on the DPDP Rules' due diligence requirement and the Colorado AI Act's impact assessment mandate, requiring independent verification that pricing algorithms do not produce discriminatory outcomes. The third

is sector-specific prohibitions on the use of sensitive personal data in pricing decisions for essential goods and services, modelled on the Maryland approach. The combination of transparency, accountability, and targeted prohibition addresses the three legal domains that surveillance pricing traverses.

For India specifically, the regulatory path forward requires three developments. The designation of major e-commerce platforms as Significant Data Fiduciaries under the DPDP Act would activate the algorithmic due diligence obligation for entities most likely to deploy surveillance pricing. The introduction of a mandatory pricing disclosure requirement under the Consumer Protection Act or the Consumer Protection (E-Commerce) Rules would address the transparency deficit. The strengthening of the CCPA's enforcement capacity, including dedicated technical expertise for investigating algorithmic pricing practices, would bridge the gap between legislative ambition and regulatory effectiveness. India co-chaired the Paris AI Action Summit in February 2025 and hosted the India AI Impact Summit in New Delhi in February 2026. A country that advocates responsible AI governance internationally must demonstrate equivalent consumer protection at home.

Algorithmic pricing is not inherently harmful, and a regulatory framework must acknowledge that distinction. Dynamic pricing that responds to supply and demand fluctuations can enhance market efficiency and benefit consumers through lower prices during periods of low demand. The regulatory concern arises when pricing algorithms exploit personal data to extract individualised surplus from consumers who are unaware that their data is being used against their economic interests. The line between legitimate price optimisation and exploitative surveillance pricing is the central regulatory challenge of the next decade. Transparency, accountability, and targeted prohibition provide the instruments necessary to draw that line.

REFERENCES

1. Abrardi, L., Cambini, C., & Rondi, L. (2021). Artificial intelligence, firms and consumer behavior: A survey. Journal of Economic Surveys, 36(4), 969–991. https://doi.org/10.1111/joes.12455
2. American Bar Association. (2026, April 23). Overlooked state developments in AI consumer protection enforcement. Antitrust Law Section Newsletter. https://www.americanbar.org/groups/antitrust_law/resources/newsletters/overlooked-state-developments-ai-consumer-protection-enforcement/
3. Baker Botts LLP. (2026, January). U.S. artificial intelligence law update: Navigating the evolving state and federal regulatory landscape. https://www.bakerbotts.com/thought-leadership/publications/2026/january/us-ai-law-update
4. Central Consumer Protection Authority. (2023, November 30). Guidelines for prevention and regulation of dark patterns, 2023. Ministry of Consumer Affairs, Government of India.
5. Consumer Finance Monitor. (2026, May 5). Maryland targets "surveillance pricing": Is it a warning shot for AI-driven pricing across industries? https://www.consumerfinancemonitor.com/2026/05/05/maryland-targets-surveillance-pricing/
6. Consumer Protection (E-Commerce) Rules, 2020, Ministry of Consumer Affairs, Government of India.
7. Consumer Protection Act, 2019, No. 35 of 2019, Acts of Parliament (India) (as amended in 2025).
8. de Lucas López, A. P., Gorneanu, A. E., Yela Aránega, A., & Gallego Martín, L. (2026). Ethics, transparency, and consumer trust in AI-enabled pricing: Implications for sustainable technology entrepreneurship and economic policy. Sustainable Technology and Entrepreneurship, 5(2), Article 100131. https://doi.org/10.1016/j.stae.2026.100131
9. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India).
10. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India (notified 13 November 2025).
11. Federal Trade Commission. (2025, January 17). FTC surveillance pricing study indicates wide range of personal data used to set individualized consumer prices [Press release]. https://www.ftc.gov/news-

events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer

12. Frazier, T. (2025, February 24). A modern consumer bill of rights in the age of AI. The Regulatory Review. https://www.theregreview.org/2025/02/24/frazier-a-modern-consumer-bill-of-rights-in-the-age-of-ai/
13. Global Competition Review. (2025, September). EU competition authorities zero in on antitrust risks of algorithmic pricing. https://globalcompetitionreview.com/guide/digital-markets-guide/fifth-edition/article/eu-competition-authorities-zero-in-antitrust-risks-of-algorithmic-pricing
14. Gunderson Dettmer. (2026, February 5). 2026 AI laws update: Key regulations and practical guidance. https://www.gunder.com/en/news-insights/insights/2026-ai-laws-update-key-regulations-and-practical-guidance
15. IAPP. (2026, February 17). India's CCPA guidelines on dark patterns: Welcome signal, but law is still soft. https://iapp.org/news/a/india-s-ccpa-guidelines-on-dark-patterns-welcome-signal-but-law-is-still-soft
16. Inside Privacy. (2026, March 26). State lawmakers introduce new wave of personalized algorithmic pricing bills. https://www.insideprivacy.com/artificial-intelligence/state-lawmakers-introduce-new-wave-of-personalized-algorithmic-pricing-bills/
17. Legal 500. (2025). Dark patterns and market power: Evaluating the Competition Commission of India's role in regulating digital deception. https://www.legal500.com/developments/press-releases/dark-patterns-and-market-power/
18. Lexology. (2025a, November 17). Digital Personal Data Protection Rules 2025: Highlights. https://www.lexology.com/library/detail.aspx?g=8cd518f8-7b2e-4379-95bb-d91f6c873acc
19. Lexology. (2025b, November 24). India's digital personal data protection regime takes effect. https://www.lexology.com/library/detail.aspx?g=2073ac40-628f-4112-81f3-fffdfd4b8858
20. Mone, et al. (2026). AI price tags and privacy: When your data sets your price. WIREs Data Mining and Knowledge Discovery, 16(1), Article e70070. https://doi.org/10.1002/widm.70070
21. MultiState. (2026, January 14). States tackled algorithmic pricing and price transparency in 2025 (plus, what to expect this year). https://www.multistate.us/insider/2026/1/13/states-tackled-algorithmic-pricing-and-price-transparency-in-2025
22. National Law Review. (2025, November 26). India passes the Digital Personal Data Protection Rules, ushering in a new digital age in India. https://natlawreview.com/article/india-passes-digital-personal-data-protection-rules-ushering-new-digital-age-india
23. Policy Circle. (2026, April 8). India's digital marketplace needs its own AI consumer safeguards. https://www.policycircle.org/opinion/digital-marketplace-rules-india/
24. Press Information Bureau. (2023, November 30). Central Consumer Protection Authority issues Guidelines for Prevention and Regulation of Dark Patterns, 2023. Government of India. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1983994
25. 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
26. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services (Digital Services Act). Official Journal of the European Union, L 277, 1–102.
27. 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). Official Journal of the European Union, L Series.
28. S.S. Rana & Co. (2025, November 24). Effect of Digital Personal Data Protection Rules, 2025 on AI regulation. https://ssrana.in/articles/effect-of-digital-personal-data-protection-rules-2025-on-ai-regulation/
29. SK Legal Consultancy. (2025, July 31). Consumer Protection Act India: 2025 amendments explained. https://sklegalconsultancy.in/consumer-protection-act-2025/

30. Skadden, Arps, Slate, Meagher & Flom LLP. (2026, January 20). New York algorithmic pricing law enacted as other jurisdictions weigh controls on price-setting technologies. https://www.skadden.com/insights/publications/2026/01/new-york-algorithmic-pricing-law
31. TechPolicy.Press. (2026, January 15). Global digital policy roundup: December 2025. https://www.techpolicy.press/global-digital-policy-roundup-december-2025/
32. The Competition Act, 2002, No. 12 of 2003, Acts of Parliament (India).
33. WilmerHale. (2026, March 13). Personalized pricing: What business lawyers need to know. https://www.wilmerhale.com/en/insights/client-alerts/20260313-personalized-pricing-what-business-lawyers-need-to-know
34. Wu, Z., Yang, Y., Zhao, J., & Wu, Y. (2022). The impact of algorithmic price discrimination on consumers' perceived betrayal. Frontiers in Psychology, 13, Article 825420. https://doi.org/10.3389/fpsyg.2022.825420