

AI Driven Smart Grids and the Right to Privacy: Legal Challenges in Consumer Energy Data Protection

Nikita Sharma¹ & Dr. Sandeep Saini²

Abstract:

The rapid integration of AI into smart grid infrastructure has fundamentally transform how energy system collects, process and utilise consumer data. Smart metres, IoT enable devices and AI driven analytics now generate granular behavioural profiles revealing occupancy patterns, daily routine and lifestyle habits raising profound concerned about consumer privacy and the advocacy of existing legal protections. This paper examines the legal challenges post by AI driven smart grades at the intersection of energy regulation and data privacy laws. Its analysis how current framework including the GDP are in the European union and sector specific energy regulations struggle to address the scale, velocity comma and sensitivity of energy data generated by AI systems. Issue explodes include the adequacy of consent mechanism the scope of data minimization obligations algorithmic transparency and the challenges of regulating third party data sharing between energy providers and commercial entities³. The people for the Argus the traditional privacy laws doctrine when not design to content with the predictive AI interference where sensitive personal conclusion can be derived from ostensibly non sensitive energy consumption data. This gap exposes consumer to risk of surveillance, profiling and discriminatory practices without meaningful legal recourse. This paper concludes by proposing a right based regulatory framework that mandates purpose limitation, algorithmic accountability, and enhance consumer control over energy data. Bridging the divide between technology innovations and fundamental right protection is imperative as smart grid deployment accelerate globally.

Keywords: smart grids, artificial intelligence, consumer privacy, energy data protection, data minimization, algorithmic transparency.

Introduction

The modern energy sector stands at a critical convergence of technological transformation and fundamental rights. The deployment of artificial intelligence across smart grid infrastructure represents one of the most pervasive and least scrutinized expansions of data surveillance in civilian life. Unlike social media platforms or e-commerce ecosystems, where consumer awareness of data collection has grown substantially over the past decade, smart grid technologies quietly harvest intimate details of daily existence: when households wake, when they cook, whether they are home, and what devices they operate. This data, generated continuously and at scale, forms the empirical foundation upon which AI systems optimize energy distribution, predict demand, and, increasingly, draw inferences about consumer behavior for commercial exploitation.

Smart grids are no longer a futuristic abstraction. As of 2024, the European Union has mandated smart meter deployment in member states under the Electricity Directive (2019/944/EU), with penetration rates exceeding 80% in Sweden, Finland, and Italy. In the United States, the Federal Energy Regulatory Commission (FERC) and state public utility commissions have encouraged smart grid investments under the Energy Independence and Security Act of 2007, resulting in over 111 million smart meter installations nationwide⁴. In India, the Government's Revamped Distribution Sector Scheme (RDSS) targets the installation of 250 million smart prepaid meters by 2025-26, making it one of the largest smart metering programmes in the world. Administered through Energy Efficiency Services Limited (EESL) and Distribution Companies (DISCOMs), the National Smart Grid

¹ PhD Scholar, Geeta Global School of Law, Geeta University

² Associate Professor & Head, Geeta Global law School, Geeta University

³ Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

⁴ Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on Common Rules for the Internal Market for Electricity, 2019 O.J. (L 158) 125.

Mission (NSGM) has already enabled deployments across Uttar Pradesh, Bihar, Rajasthan, and Delhi, raising urgent but underexamined questions about consumer data privacy under the nascent Digital Personal Data Protection Act, 2023. The Global Smart Grid Federation estimates that worldwide smart meter deployments will surpass 2 billion units by 2030, with corresponding growth in AI-driven demand response and grid optimization systems⁵.

Yet the legal infrastructure governing this data revolution has not kept pace. Privacy law in most jurisdictions was constructed around paradigms of discrete, identifiable data collection medical records, financial transactions, telephone intercepts. The emergent problem of AI inference where personal conclusions of extraordinary sensitivity are derived from seemingly mundane consumption data falls into a doctrinal lacuna that existing regulatory regimes are ill-equipped to address. A smart meter reading every fifteen minutes does not, on its face, constitute sensitive personal data. But when subjected to machine learning analytics, those readings can reveal whether a home is occupied, identify medical equipment usage, and even estimate household income with statistical precision.

Smart Grid Architecture and AI-Driven Data Analytics

A smart grid constitutes a networked electricity delivery system that integrates digital communication technologies with traditional power infrastructure to enable bidirectional flows of both electricity and data. Its core components include Advanced Metering Infrastructure (AMI) encompassing smart meters capable of recording consumption data at intervals as granular as one minute alongside IoT-enabled sensors embedded throughout transmission and distribution networks, automated demand response systems, and centralized data management platforms. These elements collectively produce what industry practitioners term the "data exhaust" of modern energy consumption: an unceasing stream of behavioral signals transmitted to utility servers and, increasingly, to cloud-based analytical platforms.

The integration of AI and machine learning into this infrastructure has qualitatively transformed the nature of data processing. Neural networks trained on consumption datasets can perform Non-Intrusive Load Monitoring (NILM) disaggregating aggregate household energy use into appliance-level consumption profiles with accuracy rates exceeding 85% in controlled trials. Predictive algorithms model future demand at household, district, and regional levels. Anomaly detection systems identify deviations from baseline consumption patterns to flag potential equipment failures, theft, or welfare concerns. What distinguishes AI-driven analysis from traditional metering is not merely its scale but its inferential capacity: the ability to derive from consumption data conclusions about household composition, occupancy schedules, health status, and economic circumstances that the data subject has never knowingly disclosed.

The Privacy Sensitivity of Energy Data

Academic research has extensively documented the behavioral richness of smart meter data. Foundational work by Molina-Markham et al. (2010) demonstrated that fine-grained consumption records allow the identification of household occupancy with 94% accuracy and the detection of individual appliances. Subsequently, Lisovich and Wicker (2008) showed that meter readings could expose whether residents were watching television, which programs they watched, and when they slept. More recent studies utilizing machine learning have expanded inferential capabilities to include detection of electric vehicle charging which, combined with geographic information, can facilitate vehicle tracking identification of medical devices such as home dialysis machines or CPAP equipment, and estimation of household income based on appliance usage signatures.

These inferential capabilities transform energy consumption data from a billing mechanism into a continuous behavioral surveillance system. The implications extend beyond abstract privacy concerns to tangible risks of harm: discriminatory insurance pricing based on inferred health conditions, targeted advertising exploiting

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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), 2016 O.J. (L 119) 1.

lifestyle insights, manipulation of vulnerable consumers by commercial third parties, and, in extreme cases, facilitation of residential burglary through occupancy inference. The sensitivity of this data is compounded by its involuntary generation unlike social media engagement energy consumption cannot be suspended without severe consequences for daily life and by its comprehensive character: every household connected to the smart grid is simultaneously a data subject.

Existing Legal Frameworks and Their Structural Limitations

The GDPR, which entered into force across the European Union in May 2018, constitutes the world's most comprehensive data protection regime and the primary legal framework applicable to smart grid data processing within EU member states. Its principles lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability are nominally well-suited to addressing the privacy challenges of smart grids⁶. Article 4(1)'s broad definition of "personal data" as "any information relating to an identified or identifiable natural person" encompasses smart meter readings, particularly given the ease with which energy consumption records can be associated with specific addresses and their residents.

The GDPR's adequacy, however, is undermined by several structural features. First, the regulation's approach to consent requiring it to be freely given, specific, informed, and unambiguous under Article 7 is operationally compromised in the smart grid context. Consumers who reject data collection through smart meters may face service degradation, higher tariffs, or inability to participate in demand response programs that offer financial benefits⁷. The "freely given" criterion is thus compromised by structural dependencies that render meaningful refusal practically impossible for most households. Recital 43 of the GDPR acknowledges that consent may not be freely given when there is a significant imbalance of power between the data subject and the controller a condition that characterizes the consumer-utility relationship in virtually all jurisdictions⁸.

Second, while Article 22 affords data subjects rights against purely automated decision-making that produces "significant" effects, this protection operates poorly against the distributed, inferential character of AI analytics applied to energy data. The relevant decisions targeted pricing, insurance risk scoring, commercial profiling may not be made by the utility company that collected the data but by third parties who received it through data-sharing arrangements, and may not be classified as "solely automated" decisions if nominal human review is interpolated at any stage. Third, the GDPR's accountability mechanisms Data Protection Impact Assessments (DPIAs) under Article 35, Data Protection Officers, and the accountability principle under Article 5(2) impose procedural obligations without guaranteeing substantive protection against inferential privacy violations⁹.

Beyond the GDPR, the European Union has developed energy-specific privacy requirements through the Electricity Directive (2019/944/EU) and Commission Recommendation 2012/148/EU on smart meter data protection¹⁰. These instruments establish that consumers must be informed of the purposes and modalities of data collection, that access to fine-grained data should be provided to third parties only with explicit consumer consent, and that smart metering systems must comply with Union data protection and privacy rules. However, these provisions largely restate GDPR principles rather than extending them, and their implementation across member states has been markedly uneven.

⁶ Charalampos Efthymiou & George Kalogridis, Smart Grid Privacy via Anonymization of Smart Metering Data, in IEEE SmartGridComm (2010).

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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), 2016 O.J. (L 119) 1.

⁸ Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

⁹ Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on Common Rules for the Internal Market for Electricity, 2019 O.J. (L 158) 125.

¹⁰ 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 1689).

In the United States, no federal privacy statute of general application governs smart grid data. The sector is regulated through a patchwork of instruments: FERC Order 745 on demand response, state public utility commission rules, and privacy policies voluntarily adopted by utilities. California has led the nation through the California Consumer Privacy Act (CCPA) and its amendment (CPR), supplemented by state utility-specific rules requiring consent for sharing of energy usage data with third parties. The National Institute of Standards and Technology (NIST) Interagency Report 7628 provides a cybersecurity framework that addresses privacy as a component of security but does not impose substantive limitations on data uses. The Federal Trade Commission's authority over unfair or deceptive trade practices offers residual oversight but has been inconsistently applied to energy sector actors¹¹.

Outside the EU and United States, regulatory development is largely nascent. China's Personal Information Protection Law (PIPL) of 2021, modeled in part on the GDPR, applies to energy data but coexists with state surveillance imperatives that substantially qualify its protections. India presents a particularly instructive case. The Digital Personal Data Protection Act, 2023 (DPDPA) enacted in August 2023 but awaiting full operationalisation constitutes India's first comprehensive data protection statute¹². While the DPDPA adopts broadly GDPR-influenced principles of purpose limitation, consent, and data minimisation, it contains significant carve-outs: Section 17 grants sweeping exemptions to government instrumentalities on grounds of national security and public order, which could extend to state-owned DISCOMs and the NSGM. Additionally, the DPDPA does not classify energy consumption data as a "special category," leaving AI-driven inferences about health, religion, or economic status derived from smart meter data without heightened protection¹³. The Electricity Act, 2003 and CERC/SERC regulations contain no meaningful consumer data privacy provisions, creating a regulatory lacuna precisely as the RDSS accelerates mass smart meter deployment. The Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) which unanimously recognised privacy as a fundamental right under Article 21 of the Constitution provides a constitutional foundation for reform, but its translation into energy sector regulation remains unrealised¹⁴. The resulting global regulatory landscape is fragmented, with advanced smart grid deployment frequently outpacing the development of meaningful privacy protections.

Principal Legal Challenges

Consent occupies a foundational role in liberal data protection theory, premised on the notion that individuals can meaningfully authorize or withhold authorization for the processing of their personal information. This theory is structurally undermined in the smart grid context. The deployment of smart metering infrastructure is typically mandated by regulatory directive or utility policy, with individual opt-out options that are practically unavailable, economically penalized, or technically circumscribed. The UK's Smart Metering Implementation Programme, for example, technically permits consumers to decline a smart meter but creates financial disincentives through differential tariff structures that, in practice, coerce acceptance. In India, the challenge is even more acute: the RDSS framework provides no meaningful opt-out, and DISCOMs embed broad data authorisations in standard-form agreements that low-income consumers are ill-equipped to contest. The DPDPA's requirement of free and informed consent under Section 6 is rendered nominal where refusal risks disruption of electricity supply a consequence of particular severity for households dependent on subsidised connections under the SAUBHAGYA scheme¹⁵.

Even where consent is formally obtained, its quality is profoundly compromised by cognitive and informational asymmetries. Privacy notices issued by utilities routinely fail to disclose the full range of inferences that AI systems will derive from consumption data, partly because those inferences are generated by complex models

¹¹ Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (FTC Report 2023)

¹² Rahul Matthan, *Beyond the Personal Data Protection Bill: Towards a Comprehensive Data Governance Framework for India* (Takshashila Institution Discussion Document 2020).

¹³ Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code

¹⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

¹⁵ Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code

whose outputs are not fully predictable at the point of consent. The concept of "informed" consent presupposes that the data subject can comprehend the uses to which their data will be put; where those uses are determined by machine learning systems trained on evolving datasets and deployed for purposes that may be redetermined over the data lifecycle, prior informed consent is structurally incoherent.

Scholars including van der Sloot (2014) and Rouvroy and Berns (2013) have argued persuasively that the consent mechanism, as currently construed in data protection law, is inadequate for algorithmic environments precisely because it treats privacy as a bilateral transaction between a data subject and a data controller, whereas AI-driven inference operates in a networked, relational context in which the privacy implications of individual data collection are substantially determined by its aggregation with data from thousands of other subjects¹⁶. This "group privacy" dimension the collective exposure created by machine learning operating across population-level datasets is not addressed by individual consent frameworks.

The data minimization principle enshrined in GDPR Article 5(1)(c) as the requirement that personal data be "adequate, relevant and limited to what is necessary" represents a second axis of tension between AI-driven grid analytics and privacy law. The optimization of AI systems is functionally dependent on maximal data collection: more granular data, collected at higher frequency, enables more accurate demand prediction, anomaly detection, and behavioral modeling. The commercial and operational imperatives of AI-driven smart grids thus run directly counter to the legal requirement of minimal data collection.

This tension is not merely theoretical. The shift from monthly meter reading to fifteen-minute interval data increasingly being replaced by one-minute or even sub-minute recording in advanced AMI deployments represents an exponential increase in the behavioral granularity of collected data, justified by utilities as necessary for real-time demand response and grid balancing. Yet studies by Quinn (2009) and Efthymiou and Kalogridis (2010) have demonstrated that many of the core operational purposes of smart grids billing, distribution planning, infrastructure maintenance can be accomplished using significantly less granular data than utilities currently collect¹⁷. The commercial exploitation of high-resolution data by utilities and their third-party partners thus inflates collection requirements beyond what legitimate grid management necessitates.

Privacy-preserving technical alternatives exist but remain under deployed. Differential privacy techniques which inject calibrated statistical noise into datasets to prevent individual identification while preserving aggregate utility have been applied successfully in other large-scale data contexts and could be adapted to smart grid analytics. Federated learning architectures, in which AI models are trained on data that remains resident on consumer devices rather than being centralized, offer another technical pathway to operationally useful AI without comprehensive data extraction¹⁸. The failure to mandate such privacy-by-design approaches in existing regulatory frameworks constitutes a significant legal gap.

The opacity of AI systems their character as "black boxes" that produce outputs whose relationship to inputs cannot be readily explained poses fundamental challenges to principles of transparency and accountability in data protection law. GDPR Articles 13 and 14 require data controllers to provide "meaningful information" about the logic of automated processing; Article 22 grants a right to explanation for consequential automated decisions. These provisions presuppose a degree of model interpretability that state-of-the-art deep learning systems do not readily provide. A neural network trained to infer household occupancy from consumption patterns may achieve high predictive accuracy through weight distributions across millions of parameters that no human reviewer can meaningfully audit.

The interpretability challenge is compounded in the smart grid context by the multi-layered architecture of AI deployment. Utilities typically do not develop AI systems in-house but procure them from technology vendors who treat model architecture as proprietary intellectual property. The data controller (the utility) may thus be

¹⁶ Antoinette Rouvroy & Thomas Berns, *Governing Without Norms: Algorithmic Governmentality and the Dehumanization of Law*, 20 *Philosophy & Technology* 45 (2013).

¹⁷ Gautam Bhatia, *Privacy and the Constitution* (Oxford Univ. Press India 2021).

¹⁸ International Energy Agency, *Digitalization and Energy* (IEA Report 2023).

legally responsible for explaining AI-driven decisions while lacking the technical capacity or contractual right to access the information necessary to provide such explanations. Data protection authorities in Germany, France, and the Netherlands have issued guidance acknowledging this gap but have not developed regulatory solutions adequate to its scale.

The EU AI Act (Regulation (EU) 2024/1689), which entered into force in August 2024, partially addresses this challenge by establishing transparency obligations for high-risk AI systems and imposing obligations of human oversight, technical documentation, and logging. The AI Act's classification of certain AI applications as "high-risk" including systems used in critical infrastructure such as energy is directly relevant to smart grid analytics. However, its practical implementation remains nascent, and the relationship between the AI Act's transparency requirements and the GDPR's right to explanation has not yet been definitively resolved by regulatory guidance or case law. India has no equivalent instrument: the DPDPA, 2023 contains no algorithmic transparency obligations, and neither CERC nor any SERC has issued guidance on AI accountability in Advanced Metering Infrastructure systems¹⁹. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 address algorithmic transparency only in the context of social media intermediaries, leaving smart grid AI entirely unregulated from a transparency standpoint.

The architecture of smart grid data governance creates structural incentives for the commercialization of consumer energy data beyond its original collection purposes. Utilities face regulatory pressure to reduce operational costs while investing in grid modernization; the monetization of consumer data through sharing agreements with technology companies, insurers, retailers, and financial institutions offers a revenue stream that offsets these costs. In many jurisdictions, the legal architecture governing such arrangements is inadequate.

Research by the Rocky Mountain Institute (2022) and the Future of Privacy Forum (2021) documented extensive third-party data-sharing practices among US utilities, including arrangements under which energy consumption data is shared with insurance companies for risk modeling, retailers for targeted advertising, and real estate platforms for property valuation. In many cases, these arrangements are authorized through broad consent provisions buried in service agreements rather than specific, granular consent for each secondary use. The GDPR's purpose limitation principle requiring that data be collected for specified, explicit purposes and not further processed in incompatible ways is frequently breached in practice, though enforcement actions against utilities have been rare²⁰.

A particularly acute concern involves the sharing of energy data with law enforcement authorities. The UK Supreme Court's decision in *Investigatory Powers Commissioner's Office v. Liberty* (2019) and the US Supreme Court's reasoning in *Carpenter v. United States* (2018) recognizing that prolonged collection of location data constitutes a search requiring a warrant have implications for the legal treatment of smart meter data sharing with law enforcement²¹. Yet the doctrinal translation of these principles to energy data has been incomplete, and utilities in many jurisdictions share consumption data with law enforcement under administrative subpoenas that do not require judicial authorization²².

The Challenge of Predictive AI Inference: A Doctrinal Gap

The most profound legal challenge posed by AI-driven smart grids may be the one least addressed by existing doctrine: the capacity of machine learning systems to derive sensitive personal conclusions from data that is not, in isolation, classified as sensitive. Privacy law in most jurisdictions draws categorical distinctions between ordinary personal data and "special categories" of sensitive data revealing racial origin, health status, political opinions, religious beliefs, and sexual orientation to which heightened protections apply. These distinctions were developed in a pre-AI context, where the sensitivity of data was assumed to inhere in the data itself.

¹⁹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

²⁰ R. Prasad & V. Sridhar, The Emerging Aadhaar-Smart Grid Nexus: Data Convergence and Privacy Risks in India's Digital Infrastructure, 18 Indian J. L. & Tech. (2022).

²¹ *Carpenter v. United States*, 585 U.S. 296 (2018).

²² *Carpenter v. United States*, 585 U.S. 296 (2018).

AI inference dissolves this ontological assumption. Smart meter data does not reveal, on its face, whether a household member has diabetes, holds religious beliefs that require nighttime prayer, or is engaged in a same-sex relationship. Yet each of these inferences can be drawn from consumption patterns with statistical confidence by appropriately trained models: insulin pump operation generates characteristic consumption signatures; nocturnal prayer is associated with distinctive appliance use patterns; household composition inferences enabled by NILM can expose the presence of same-sex partners²³. When AI processing transforms non-sensitive data into sensitive inferences, the categorical architecture of existing privacy law provides no protection because the sensitive inference is not, legally, "data" that was "collected" it is an algorithmic output.

This gap in doctrinal coverage has been recognized by scholars including Solove (2013), who argues that the aggregation of individually innocuous data into sensitive profiles represents a distinct privacy harm the "aggregation problem" not captured by classical privacy frameworks focused on intrusion, disclosure, or deception. The European Data Protection Board's Guidelines 05/2022 on consent and processing of special categories take a step toward addressing this by suggesting that inferred data falling within special categories should be treated as special category data. However, this guidance has not been translated into binding regulation, and its scope and application in the smart grid context remain contested²⁴.

The discrimination risks arising from AI inference in smart grids are substantial. Insurance companies armed with energy consumption profiles can segment customers by inferred health risk or lifestyle, effectively circumventing prohibitions on the use of sensitive data in underwriting. Employers who access smart meter data through data broker intermediaries can make hiring decisions informed by inferred personal characteristics. Financial institutions can deny credit based on inferred income instability derived from unusual consumption patterns during periods of likely unemployment. These scenarios are not hypothetical: investigative journalism in the United States has documented the availability of consumer energy data through data broker markets that aggregate utility disclosures, and the Federal Trade Commission's 2023 data broker report documented the sale of energy consumption data as a component of consumer profiles marketed to insurers and employers. In the Indian context, these risks are compounded by the scale of financial exclusion: AI inference from smart meter data held by DISCOMs, when shared with fintech lenders or microfinance institutions, could generate discriminatory credit-scoring proxies that disadvantage rural and low-income consumers who lack the means to challenge or even identify such profiling. The absence of any sectoral prohibition on such sharing in the Electricity Act, 2003 or DPDPA, 2023 renders this a live and largely unaddressed threat²⁵.

Conclusion

AI-driven smart grids represent both a technological achievement of extraordinary potential benefit and a privacy challenge of commensurate scale. The capacity to optimize energy distribution, reduce carbon emissions, integrate renewable generation, and empower consumers to manage their energy use are genuine public goods that justify substantial investment in smart grid infrastructure. But these benefits are not contingent upon the sacrifice of consumer privacy; they can be realized within a regulatory architecture that treats privacy protection not as an obstacle to technological progress but as a condition of its legitimacy.

The legal challenges examined in this paper inadequate consent, insufficient data minimization, algorithmic opacity, and unregulated commercial data exploitation are not inevitable consequences of smart grid technology. They are consequences of regulatory frameworks designed for a pre-AI world that have not been updated to address the inferential power of machine learning applied to continuous behavioral data. The GDPR, for all its ambition, was not architected to govern the intersection of IoT mass surveillance and predictive AI that characterizes contemporary smart grid deployment.

²³ Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013).

²⁴ European Data Protection Board, Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement (2022).

²⁵ Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament (India).

The reforms proposed in this paper enhanced purpose limitation, algorithmic accountability through mandatory auditing, affirmative consumer control, and international regulatory coordination are technically feasible, legally grounded in existing rights-based frameworks, and consistent with the operational requirements of modern energy systems. Their implementation requires political will from legislators, regulatory initiative from energy and data protection authorities, and technical commitment from utilities and AI vendors. The stakes are commensurate: in a world of ubiquitous smart grid deployment, the right to privacy in one's home is inseparable from the right to privacy in one's energy consumption.

As the global energy transition accelerates and AI systems become more deeply embedded in grid infrastructure, the window for designing privacy protections into the architecture of these systems rather than attempting to retrofit them after deployment is narrowing. The moment for regulatory action is now, before the data governance defaults of early smart grid deployment become entrenched technical and commercial realities that resist legal reform. The history of digital privacy regulation from the failure to govern social media data before it shaped democratic discourse, to the inadequacy of financial data protections before algorithmic credit scoring transformed access to economic opportunity counsels' urgency. Smart grids must not repeat these failures.