International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 26-02-2026, Accepted: 29-03-2026, Published: 13-04-2026
Volume 12, Issue 2, 2026, Page No. 69-75

The Internet of Things (Iot) and its legal limitations: A comparative analysis of Indian and United States legal frameworks

Janhvi Bhushan Mishra[1], Dr Juhi saxena[2]
[1] Amity law school, Amity University, Lucknow, Uttar Pradesh, India
[2] Assistant Professor, Amity law school, Amity University, Lucknow, Uttar Pradesh, India

Abstract
The fast development of the Internet of Things (IoT) has transformed the current digital ecosystems because this phenomenon allows connecting devices, sensors, and embedded systems in a seamless way. Nevertheless, such an unprecedented growth has brought forth serious legal, ethical and regulatory issues. The study looks at the legal constraints of IoT, comparatively in both India and the United States, and some of the aspects addressed in the context of data protection, privacy, cybersecurity, profiling, surveillance, and cross-border data governance.
The legislature in India is based on the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, yet both frameworks do not provide any obligations to the IoT sector, interoperability standards, or sector-wide protection against automated decision-making and profiling. The sectoral regulations, e.g., the M2M guide lines of TRAI, Smart Cities Mission strategies, and regulations of health-tech, are disjointed and ineffective.
The US, conversely, does not enforce a federal statute on data privacy, and instead falls upon a network of sectoral laws, including the FTC Act, the HIPAA, the COPPA, the GLBA, and state legislation like the California Consumer Privacy Act (CCPA) and the California IoT Security Law. This creates a problem of unequal protection of regulations within industries and jurisdictions even though some states have more robust security requirements and protection on privacy.
The comparative analysis shows that India enjoys the advantages of a single national privacy law, but its enforcement measures and recommendations regarding the IoT are not yet well-developed. In the meantime, the U.S. is more mature in the device-level standard of security but does not have consistent national regulations on the data practice, profiling, and cross-device surveillance. The paper concludes by stating that regulatory gaps in both countries are huge and there should be unified IoT governance systems, obligated security measures, and enhanced tools of accountability to mitigate the new threats in a more globalized world.

Keywords: Internet of Things (IoT), digital ecosystems, data protection, privacy, cybersecurity, legal frameworks, regulatory challenges, automated decision-making

Introduction
Internet of Things (IoT) has become one of the most disruptive technological systems of the twenty-first century that has radically changed the interaction between individuals, organizations and governments with the digital world. IoT is a massive structure of interwoven devices, including smartphones, sensors, wearables, smart appliances, industrial robots, surveillance systems and autonomous machines, that can collect, process, and communicate real-time information using embedded technologies. With these devices entering more sectors of the economy, including healthcare, transportation, agriculture, manufacturing, the government, and personal lifestyle, the Internet of Things has developed as something futuristic to an aspect of current digital infrastructure. With the growth of high-speed internet, artificial intelligence, affordable sensors, and cloud computing, the application of IoT is expanding at an unprecedented rate, with new opportunities of automation, efficiency, predictive analytics, and data-driven decisions.
Nonetheless, as much as IoT offers economic growth and improved quality of life, it is also associated with deep legal, ethical, and regulatory issues that the current laws are finding difficult to control. IoT produces a persistent and ubiquitous stream of granular personal and behavioural data in contrast to the conventional technologies. There are numerous IoT gadgets that run quietly in the background, gathering data regarding the user movement, habits, health indicators, discussions, emotional trends, and a routine-often without their prior or fully-informed approval. It gives rise to a number of serious issues like the unauthorized gathering of data, profiling, algorithmic decision-making, transparent third-party data disclosure, and 24-7 surveillance using wearables and sensors installed at home. In addition, the IoT devices have weak security features and are therefore very susceptible to cyberattacks, ransomware, identity theft, and massive data breaches as witnessed with the Mirai botnet attack.
These predicaments reveal substantial lapses in law systems. Traditional computing technologies designed laws are usually ineffective when dealing with high-layered, cross-border, and machine-driven IoT data streams. The absence of uniform privacy practices, undefined liability systems, inconsistent consent conventions and the jurisdictional issues makes it difficult to regulate. This has rendered governments of the world especially in India and the United States to be under extreme pressure in developing laws that are able to address individual rights in a comprehensive manner and yet enhance technological progress.
India has a legal attitude towards IoT that is defined by the act of Information Technology Act, 2000 [9], and the Digital Personal Data Protection (DPDP) Act, 2023 [10]. These laws might solve some part of privacy and cybersecurity, but lack the IoT-specific guidelines and cannot be enforced because

of the constraints of the devices they apply to, the cross-border flow of data, and the intricacy of the IoT architectures. The US, however, does not have a single law on Federal data protection but rather a disjointed network of sector legislation and Federal Trade Commission (FTC) regulations and state legislation, such as the California Consumer Privacy Act (CCPA) and the California IoT Security Law. This has the effect of creating skewed consumer protection with high protection standards in some states and low or absent protection standards in others.

Therefore, IoT is a place where technological innovation and uncertainty in legislation meet. India and the United States show that the two countries have similar challenges, as well as unique regulatory methods in terms of tech laws. Recognizing these differences is important in drawing the loopholes in the current legislation and preparing holistic, IoT-specific models that have the capacity to mitigate the emerging threats. With the growth of IoT in the most vital areas, now more than ever, legal protection is required to safeguard privacy, security, accountability, and the ethical application of data in a more connected world.

Background of IoTs

The Internet of Things concept was coined by Kevin Ashton in 1999 but the theoretical underpinnings of IoT trace to the emergence of microcontrollers, wireless network, telemetry systems, and early machine-to-machine (M2M) communication technologies. Development of IoT is a result of decades of computer, communication, automation and sensor engineering advancement.

IoT started to take off as Radio Frequency Identification (RFID) tags became commonly used in supply chain management, allowing the physical objects to be uniquely identified and tracked. The shift of RFID based tracking to smart, connected devices brought about through low-power processor development, embedded operating systems and the growth of the internet in the early 2000s. With the availability of mobile internet, 4G networks, and cloud computing, the size of IoT implementation increased manifold.

IoT is technically a combination of several different fields: embedded systems, big data analytics, cloud computing, edge computing, artificial intelligence, and ubiquitous networking. These technologies enable the IoT devices to collect real-time information around them, process the information on their own, and communicate with other devices or servers without human intervention. Developments like smart factories in Industry 4.0, intelligent healthcare, autonomous vehicles, intelligent grids, precision agriculture, and environmental monitoring are possible due to this capability.

The expansion of the IoT ecosystem has been significantly contributed by the cost reduction in hardware and the reduction in miniaturization of devices. Sensors that were previously costly and had limited capabilities are now inexpensive, energy efficient and highly connected. Likewise, cloud-based solutions by Amazon, Google, and Microsoft have enabled organizations to store, analyze, and process large quantities of data that are being produced by IoT systems. The transition to edge and fog computing further cuts down latency and boost systems autonomy of IoT devices by allowing them to process data where they are or close to it.

IoT has been on the rise both in developed economies and developing economies worldwide. In developed industrialized countries such as the United States, IoT has entered the system of transportation, healthcare, aviation, defense, and manufacturing with an extensive digital infrastructure. In developing economies including India, IoT is a major factor driving economic modernization because of efforts such as Digital India, Smart Cities Mission, and the development of low-cost mobile internet.

The socio-economic effect of IoT is serious. Its benefits to business include automation and predictive analytics to improve the efficiency of the business, smart resource management to help businesses stay environmentally sustainable, and smart homes and wearable technology to simplify daily life. IoT-based systems (IoT technologies) allow farmers to monitor the soil, remotely monitor patients in hospitals, governments to monitor traffic and pollution, and industrial enterprises to predict maintenance and reduce downtime.

Nevertheless, along with this fast growth comes a complicated terrain of problems. IoT is interconnected, which intensifies the risk of cyberattacks, information breaches, and misuse of personal information. Most IoT devices are not well secured, are not standardized and are usually running on old firmwares. Also, data ownership, data sovereignty, surveillance, and ethical governance are also issues that are questioned by the sheer volume of data that is being produced. The world is now struggling with policymakers developing laws and regulatory frameworks that would provide the security, privacy, interoperability and accountability in the IoT ecosystem all whilst permitting technological innovation.

In this way, the history of the IoT is not a history of technological development, but it is also a history of changing the world. It acknowledges that a middle ground is needed to support the innovation and mitigate the legal constraints, cybersecurity threats and the regulatory concerns that come with its high-speed expansion.

Key Legal and privacy concerns in IoT.

The high rate of the development of Internet of Things (IoT) devices has transformed connectivity, automation, and real-time data production. Nevertheless, there is another aspect of this interconnected ecosystem: it introduces a set of legal, privacy, and ethical issues. With the emerging trends of billions of devices gathering, processing, and transmitting personal and non-personal information, jurisdiction problems have ensued that intersect privacy rights, cybersecurity, consumer protection, and data governance. The subsequent sections develop major legal and privacy issues that are emerging as a result of the adoption of the IoT, and contrast the approaches of India and the U.S to the emerging issues.

After accessing the wireless network, the auditor was able to gather data without authorization from the user.

Unauthorized Data Collection The auditor accessed the wireless network and collected data without user authorization.

Unauthorized or excessive data collection is considered one of the biggest problems in the ecosystem of the IoT. IoT devices, including smart home assistants, fitness trackers, security cameras, smart TVs, and connected vehicles and home appliances, generally collect data in the back of mind and do not always require the explicit attention of the user.

In contrast to traditional digital platforms, IoT gadgets typically do not have displays or user-friendly interfaces, and users can hardly know what kind of data is being gathered, processed, or moved. The sensors installed in the IoT devices can constantly monitor the environmental conditions and behavioral patterns, biometric indicators, and location information, forming a databank of the everyday life of the person.

In India, the Digital Personal Data Protection (DPDP) Act, 2023 [10] proposes a consent-based framework, where the company must receive clear and affirmative consent to collect personal data. Nevertheless, the Act is not yet specific in terms of granular guidance on what exactly the IoT ecosystems present, namely the autonomous/passive operation of the devices. This creates a pragmatic enforcement gap: despite the law imposing the need to have an informed consent, the IoT device architecture renders meaningful consent virtually impossible. In the meantime, the United States assumes mostly a sectoral approach to regulation, and legislation, including HIPAA, COPPA, and the FTC Act, regulates one sector or unfair methods. Nevertheless, a centralized, federal law on data protection that can be implemented across the board on IoT manufacturers does not exist. This leads to a situation where companies have few limitations on how they will gather, consolidate, and monetize consumer data using IoT devices, unless the data is in a regulated category.

In this way, India and the U.S. are having a difficult time trying to contain pervasive, ambient surveillance via IoT. The lack of unified disclosure standards, disclosure at a device level and easy to use privacy features worsens the problem further.

Profiling and Behavioral Tracking.

IoT devices generate streams of data on a constant basis, and it is possible to profile the behaviour. As an illustration, smartwatches are able to monitor sleep patterns, heart rate and movement; smart speakers, voice patterns and commands; smart home, day to day routines. When aggregated and processed with the help of predictive analytics or artificial intelligence, these data points can tell personal information about their lifestyle, health condition, financial behaviour, or mental habits. This profiling may be applied towards making automatic decisions or it may be applied in order to manipulate consumer behavior- not always openly.

In India, despite the fact that the Puttaswamy case declared by the Supreme Court recognised privacy as a basic right, there exists no direct law that is specifically set on governing behavioural profiling . DPDP Act is addressing the personal data, but does not provide a clear definition of the scope of the algorithmic profiling, automated decision-making, or discriminatory outcomes of the data produced by the IoT. This creates considerable grey areas with regard to consumer protection and autonomy of data.

On the contrary, the United States allows widespread profiling of data through its market-driven regulation. User data are frequently used by the private companies to provide more personalized ads, change insurance rates, modify credit products, or determine the interests of the consumer. Although the FTC is able to interfere in situations involving unfair or deceptive practices, it does not actually regulate profiling. Industry specific legislation does offer certain safeguards (such as the Fair credit reporting act in finance), but they remain incomplete with respect to algorithmic profiling on the basis of IoT ecosystems. As a result, people are likely to be treated differently without their knowledge during employment screening, insurance rates, or targeted advertisement. Both jurisdictions are thus struggling with the need to balance the innovation with protection against discriminatory or black-box analytics.

Transparent Exchange of Data between Companies

One of the typical characteristics of the IoT ecosystem is the exchange of gathered information between a large chain of intermediaries. The IoT manufacturers regularly send user information to the cloud service providers, data brokers, third-party analytics partners, advertising networks, insurance companies, and even government agencies. Such flows of data are not always visible to end users and they are hardly vulnerable to any significant consent.

The DPDP Act in India compels the data fiduciaries to reveal the intent of data sharing, and it does not specify the elaborate transparency of who downstream recipients of data are, and whether it is being transferred across the border. Also, the enforcement mechanisms are not well developed yet, and the Act does not have any detailed audit demands, which would require manufacturers of data-gathering devices to pay attention to secondary data usage. This creates a disjointed and loosely controlled space, in which users themselves have no ability to trace the route that their IoT data takes through private operators.

The United States does not have a federal privacy law and this has enabled firms to take up extensive data-sharing initiatives. Businesses tend to make use of privacy policies that are long and complicated in order to justify such transfers. Even in cases where disclosure has been made, the consumers do not read or comprehend them. Although rights to know, delete, or opt out of the sale of data are introduced in California Consumer Privacy Act (CCPA) and followed by the CPRA, the legislation is restricted within certain states. This has led to most of the country being under poor and unequal standards. In both jurisdictions, the lack of transparency in data-sharing processes compromises autonomy and renders accountability very hard.

Ineffectual or Fraudulent Consent Makes

As a legal foundation of data processing, consent is near meaningless in the context of the IoT given the design limitations. A majority of the IoT devices have users to agree to pre-written agreements lengthy to read during activation or setup. Such contracts tend to be vaguely or excessively broad to allow wide-reaching data collection, surveillance of behaviour, and transfer of the data to third parties. The pre-checked consent boxes, bundled consent (refusing to consent means the device will not work) or dark patterns, which deceive the user into giving their permission without full knowledge, are used in many devices.

In India, the DPDP Act is focused on explicit, informed and freely given consent. Nevertheless, challenges of acquiring such consent with gadgets that lack appropriate interface mechanisms are not covered in the Act. This leaves a loophole in compliance in that the manufacturers can claim that the user had agreed to use the device although the process was not transparent or fair.

The old-established model of notice and choice championed by FTC is strongly criticized as being inefficient in the U.S. It imposes on the consumers the task of reading and

digesting complicated privacy policies- a far-fetched task considering the passive character of IoT technologies. In addition, consumer protection is further jeopardized by consent fatigue and dark patterns resulting in mass acceptance of terms that a majority of users do not even bother to look into. This establishes a legal field where the businesses are able to count on the procedural compliance but subvert the substantive privacy rights.

Continuous Surveillance

IoT devices are potentially dangerous in terms of surveillance because they are ubiquitous in personal and workplaces. Smart security cameras, motion sensors, voice assistants (such as Alexa by Amazon or Google Home), wearable devices with GPS capabilities, and surveillance cameras at the workplace can monitor the behaviour, movements, conversations and interactions of an individual throughout the day. This is a surveillance-by-default setting in which there is an ever-shimmering boundary between voluntary and involuntary information sharing.

In India, these problems are a constitutional issue since the Supreme Court acknowledges privacy as a fundamental right. Informational privacy, decisional autonomy, and personal dignity are possible violations of continuous surveillance. However, the existing legislation offers little protection to the concerns of IoTs. India does not have any thorough surveillance laws that govern the privately-run surveillance, surveillance at the work place, or surveillance of their homes. Consequently, the aspect of IoT-based monitoring is frequently conducted off-the-record, without a chance of judicial or regulatory oversight.

In the United States, Fourth Amendment unreasonable searches and seizures collide with surveillance issues. Nevertheless, they are mostly applied to state actors, rather than to private companies. Monitoring tools based on IoT are used more often by employers to monitor the productivity of workers, their movement, and health indicators. Although there is no standard federal regulation, there are statutes mandating the disclosure of surveillance in the workplace, which are in effect in some states. IoT devices have been used in numerous criminal cases at home, and the question of whether the data of users is considered to be a private one is debatable. On the whole, the two nations struggle to overcome the current surveillance challenges with the help of outdated legislation.

Cyberattacks and Data Breach Exposure

Cyber attacks are typically more successful on IoT devices, which are have low processing power and old-firmware and weak authentication schemes and security protocols are not standardized. The IoT devices appear to have these weaknesses, as they are useful to hackers who want to use them to get botnets, steal personal data, use them to execute Distributed Denial of service (DDoS) attacks, or to infiltrate larger networks. The 2016 Mirai botnet incident proved to have disastrous possibilities of unsecured IoT gadgets, as millions of infiltrated devices were employed to interfere with significant websites and the internet infrastructure around the globe.

In India, there is still fragmentation in laws in cybersecurity. The Information Technology Act, 2000 [9] also covers the data breaches and unauthorized access, however, it does not enforce the obligatory provisions of IoT security. Manufacturers are not required to produce secure device configuration, frequent software updates, vulnerability reporting, or certify the device security.

This is why, the Indian market has been flooded with insecure IoT products that are not regulated.

America is not any exception and has its fair share of challenges but certain states have led. Indicatively, the IoT Security Law (SB-327) enacted in California requires devices to be connected with some reasonable security features like unique passwords or authentication. Nonetheless, this criterion is ambiguous, and it is not strictly followed. Federal The IoT Cybersecurity Improvement Act does not cover consumer products at the federal level, only the devices procured by the government. This has left millions of American homes vulnerable to cyberattack by poorly secured IoT devices.

Legal Framework in India

The legal and regulatory landscape of the Internet of Things in India is still in its development and disjointed state, with the previous cyber laws, recently passed privacy laws, and fragmented sectoral regulations. Although India has been making efforts to develop a powerful data protection and technology governance framework, these structures have failed to match the sophistication and size of IoT systems. Consequently, gaps in regulatory coverage, enforcement and accountability of risks associated with IoT are very high.

Information Technology Act, 2000 [9]

The cyber legal regime in India is supported by the Information technology act of 2000 [9] (IT act). The Act, which was enacted mainly to provide legal status to electronic communications and fight cybercrime, contains unauthorized access, hacking, data theft, and damage to computer systems provisions. Section 43 and 66 punish the unlicensed access, interference, data retrieval and disruption of computer resources. Section 43A will make corporations liable in case of negligence in processing sensitive personal data. In the meantime, Section 72A prosecutes any violation of confidentiality and misuse of personal information.

Nonetheless, the IT Act was written when the IoT technology was not in existence, despite its significance. Therefore, it does not explicitly discuss the layered, autonomous, and sensor-driven character of the IoT systems. IoT devices are usually remote controlled and not directly controlled by people, passively collecting information, and practicing automatic decision-making, which are not even specified in the Act. In addition, the definition of computer resources in the Act is quite wide, yet in the technological context it is obsolete, and it is unclear whether such devices as smart household appliances, wearables, industrial robotics, or the sensor that is powered by AI qualify as the ones that are covered by the definition.

Also, the Act addresses cybercrimes but not the data governance, privacy-by-design, interoperability, device authentication, and IoT-related security requirements. The IT Act cannot be used to combat the current risks due to the introduction of AI-powered profiling and cross-device tracking. Thus, although the IT Act is a primary law, it is not a comprehensive regulatory tool of the IoT.

Digital Personal Data Protection (DPDP) Act, 2023 [10].

The DPDP Act, 2023 [10], is the first laws in India to create a national privacy in respect to the consent, user rights, and data protection norms. The principles introduced in the Act include lawful processing, minimization of data, purpose limitation and transparency. Before the collection of

personal data, the data fiduciaries should be given consent free, informed, specific and unambiguous. The users will have the rights to access, to correct, to delete their data and to appoint representatives to the data related issues.

Nevertheless, the DPDP Act is also limited in a number of ways used in terms of Internet of Things ecosystem. To start with, the Act lacks IoT-specific requirements like the fact that companies are obligated to issue device-level privacy notices or have on-device consent, or transparency requirements that can be tailored to screenless devices. Since the majority of IoT devices do not have user interfaces, it is virtually impossible to get informed consent or present notices. Manufacturers are still utilizing app-based or bundled consent models which sabotage transparency.

Second, AI-driven profiling, automated decision-making, and behavioural analytics are not explicitly regulated by the Act but are at the core of the IoT operations. In the absence of regulation of algorithmic transparency, bias, or opt-out of profiling, an individual is at risk of discrimination or black box decisions based upon IoT data.

Third, implementation is a major problem. The IoT devices are imported by various international companies whose number is large, with many ones not having physical presence or operation base in India. It becomes very hard to enforce compliance, audit or penalize in such instances. Also, the DPDP Act is yet to specify data breach notifications when using non-personal data, which is one of the main elements of the IoT analytics.

Sectoral Regulations

Telecommunication and Machine-to-Machine (M2M) Guidelines (TRAI/DoT).

The telecom regulators of India have published rudimentary guidelines to M2M communication and provisioning of SIM to IoT gadgets. These are Know Your Customer (KYC) verification requirement of embedded SIMs, licensing requirement of IoT service providers and instruction on secure communication protocols. Nonetheless, these rules are not that binding, and most of them are voluntary. They lack technical security requirements, device certification, and interoperability requirements.

Smart Cities Mission

The Smart Cities Mission, which is an initiative in India, is meant to capture the role of IoT in the governance of cities, such as traffic control, solid waste, city monitoring, and surveillance. Although the use of IoT in the public has been applied on a massive scale, no unified privacy system exists to regulate the smart city data. Cities embrace dissimilar vendor systems having diverse data security capacities. Issues relating to facial recognition, predictive policing, and centralized surveillance are not addressed yet.

Healthcare IoT Regulations

IoT finds widespread application in the healthcare industry in areas such as remote healthcare monitoring systems, telemedicine and digital diagnostics. But, the regulations are disjointed in the IT Act, the Telemedicine Practice Guidelines and the Clinical Establishments Act. It has no specific health data protection legislation. Such problems as biometric data security, interoperability, and medical IoT device certification are not strongly controlled.

Regulatory Gaps in India

India does not have an overarching and specific legislation regarding IoT that defines enforceable specifications regarding security, data security, device certification, algorithms accountability, and cross-device profiling . The current legislation offers fragmented protection that has significant loopholes in the transparency, governance, and consumer rights in the IoT ecosystem.

The United States of America is a nation with a legal framework.

The United States has a decentralized and market-based regulatory practice as opposed to that of India. There is no federal privacy law in the U.S. which creates an imbalanced protection in the industries and states. Internet of things governance thus requires both consumer protection laws, state-government efforts, and self-governing standards.

Not having a Federal Data Protection Law.

The United States does not have a national privacy law that is comparable to the GDPR or DPDP Act in the EU or India. Rather, the U.S. uses sector-based fragmented regulations. Act of Federal Trade Commission (FTC) . One of the provisions of the FTC Act is against unfair or deceptive trade practices. This authority has been exercised by the FTC to penalize firms that have insecure IoT products, deceptive privacy policies, or poor data protection practices. The power of the FTC is however reactive and not proactive. It is not able to specify certain IoT security standards or impose the privacy-by-design premises.

Health Insurance Portability and Accountability Act, HIPAA.

The HIPAA governs the privacy and security of medical information. Nonetheless, not all of the health-related IoT gadgets, including fitness trackers and wellness apps, are subject to HIPAA, as they are considered consumer products, but not healthcare services. This gives a lot of loopholes.

COPPA Children Online Privacy Protection Act.

COPPA limits the gathering of information involving children below 13 years. Nevertheless, IoT toys and smart devices do not tend to provide a proper age verification or parent consent operation.

GLBA, FCRA and Other Financial Laws.

Such regulations apply to the field of financial information but do not guard against cross-device behavioural profiling or data aggregation by IoT systems. On the whole, the lack of a single privacy law leads to unequal protection, and consumers are susceptible to surveillance and profiling, as well as ambiguous information exchange.

State-Level Laws

California Consumer Privacy Act (CCPA) and CPRA.

California is the best state in privacy regulation in the U.S. The CCPA provides consumers with rights to access to, delete, and opt out of the sale of personal data, which is of high importance to the data produced by the IoT. The California Privacy Rights Act (CPRA) enhances these protections due to the creation of laws on data brokers, restriction on profiling, and transparency of automated decision-making processes.

These protections, however, are only applicable in California, so they provide patchwork regulations nationwide.

California SB-327 IoT Security.
According to this law, manufacturers of connected devices are required to develop reasonable security functions, including unique passwords and secure authentication. Despite being an important initial step, the law does not provide detailed standards and enforcement capacity. Other states such as Oregon and Virginia have gone further to adopt such laws though this is not a consistent nationally.

Insufficiency of a general IoT regulation.
The legal system of the U.S. fails to control: cross-device profiling, IoT processors make decisions automatically, algorithmic discrimination, data broker ecosystems, AI-driven predictions, safety standards on the device level, lifecycle security (e.g., compulsory updates).
In the absence of straightforward regulations, businesses conduct a lot of behavioural analytics and uncontrolled information dissemination. Manufacturers of IoT do not have to follow the standardized cybersecurity principles, which results in vulnerabilities of the oil of the same kind as in the case of the Mirai botnet.
Although federal authorities such as NIST have published voluntary frameworks of cybersecurity on the IoT, they have not been legally enforceable. This makes consumer protections, accountability, and transparency weak.

U.S. Regulatory Gaps
The United States possesses powerful enforcement policies and powerful regulators such as FTC, but does not have a centralized statutory framework of privacy, security, and profiling of IoT. This leadership of the innovation by the private sector leads to the swift extension of IoT at the expense of the continuity of consumer protection.

Comparison between India and the United States.
Regulatory practices of the United States and India concerning the Internet of Things (IoT) have significant differences as a result of differences in the philosophies of law and institutional frameworks, as well as governance priorities through technology. India adheres to a centralized, unified model of data protection on the basis of the Digital Personal Data Protection (DPDP) Act, 2023 [10], which offers one national model to be used in personal data processing. This centralized strategy has conceptual clarity and consistent implementation across industries. The United States, by contrast, uses a disjointed model of various federal sectoral laws, including the HIPAA law on health data, the COPPA on children's data, and the FTC Act on consumer protection, along with state-level privacy laws, including the California Consumer Privacy Act (CCPA). This deviation brings about a lattice work of safeguards that differ largely among industries and geographical areas, and tend to leave loopholes in the governance of IoT.
There is also a sharp difference between the two jurisdictions with regard to consent mechanisms. The DPDP Act in India places the key role of the personal processing of data on reliance on explicit, informed, and revocable consent. Nevertheless, in reality, the internet of things frequently avoids meaningful consent because of design constraints and through feature-based or application-based approval, which diminishes the efficacy of India with its robust laws. The United States is based on the historic model of notice-and-choice, where firms offer privacy notifications and customers are considered to have given their consent through further use. The model has been highly criticized for being inadequate in IoT challenges where disclosures are complicated and user interfaces are restricted.
In the issue of profiling and behavioural analytics, India does not have any clear laws on automated decisions or algorithmic profiling. Even though the right to privacy identified in the Puttaswamy decision is theoretically constitutionally guaranteed, in the absence of specific legislative provisions, people are exposed to the black box or discriminative profiling. The US too does not fully regulate profiling, except in a few industries like finance or credit scoring. This brings about the wide latitude of freedom to companies to indulge in cross-gadget tracking and forecasting behaviour using data created by IoTs.
Another distinction is in the form of security standards. There are no specific cybersecurity requirements related to IoT in India, and general requirements are imposed by the IT Act and supported by voluntary practices. This regulatory gap is why devices that are not secured to drift through the Indian market. On the other hand, other states in the U.S. have passed laws enforcing IoT security that manufacturers have to provide so-called reasonable security features, including unique passwords or authentications on their devices. Although these laws are a good move, they only cover the state-level and do not provide uniformity on a countrywide level.
Jurisdictional differences are also brought out through surveillance issues. In India, the theoretical basis to oppose intrusive monitoring is a constitutional right to privacy. Nevertheless, the absence of a universal law on surveillance and the use of IoT in smart cities pose great chances of overreach. In the United States, the Fourth Amendment of the constitution provides rights against government searches and seizures as the basis of privacy rights. However, such protections are largely limited to the action of the state, rather than the surveillance of the private sector, which gives companies a wide margin of discretion in monitoring user activity using IoT equipment.
Policies of cross-border data flow are also radically different. The DPDP Act framework in India is shifting towards controlled data transfers, where the government has the authority to inform the international data transfer about trusted jurisdictions. This is an indication of a more conservative and sovereignty-consciousness. The US, in its turn, adheres to a laissez-faire paradigm according to which free cross-border data transfers are relatively permissible because of its market-oriented regulatory school of thought and high dependence on multinational clouds.
On the whole, a comparative evaluation allows concluding that India has a coherent and dynamic law on data protection but is problematic with enforcement, particularly in device-based ecosystems such as IoT. The US is more secure in some states, and its enforcement institutions are more mature and developed, yet its inability to exercise national consistency and the lack of a federal privacy law add to the fragmentation of the regulations.
This comparison reveals the most important conclusion: India has a higher degree of centralized privacy protection, though it does not implement it specifically on the IoT; the U.S. has superior norms of state security, but does not have national regulation of this issue.

Conclusion

The development of the Internet of Things is one of the most radical technological changes of the 21st century that allows reaching new heights of automation, efficiency, and data-driven decision-making. These advantages, however, come with huge legal, ethical, and security issues that the current regulatory processes in both India and the United States are unable to effectively tackle. This study shows that despite the fact that both jurisdictions acknowledge the increasing necessity of mechanisms of IoT governance, their methods are quite different, which has significant advantages and serious flaws.

The centralized legislation that India is bound to includes the Information Technology Act, 2000 [9], and the Digital Personal Data Protection Act, 2023 [10], which are associated with the legal system of this country. Although these laws have provided a backbone framework on data protection and cybersecurity, no IoT-specific background or strong safeguards on profiling, automated decision-making, or machine-to-machine communications (M2M) communications are done.

There is also uneven enforcement, especially in industries such as smart cities, the healthcare Internet of Things, and consumer electronics in which privacy requirements are divided or nonexistent. India has a risk of increasing the disparity between technology usage and consumer protection unless there is an in-depth enforceable regulation of IoT.

America, however, has a sectoral and decentralized system of regulation. Although no federal law centers on data protection, state based legislation, particularly in California has brought about serious improvements to the consumer rights as well as the protection of the device. However, the disadvantage of this blocked model is that it creates different state-specific and industry-specific protections.

Other major concerns, including cross-device profiling, data brokerage, and surveillance, are still uncontrolled sufficiently, which creates tremendous gaps in an environment that is becoming more and more dominated by interconnected devices.

The comparative results reveal that the two countries have significant regulatory blind spots. India needs more mechanisms and IoT-oriented laws, whereas the U.S. should have national consistency and overall federal standards. To protect the rights of consumers and limit the threats produced by the system, a unified regulatory framework, including the requirements associated with the security of the devices, the increased level of consent, the disclosure of the profiling requirements, and the equal data protection standards, is needed .

Finally, the study enriches the existing discussion on the subject of technology law by formulating the essentials without any legal gaps in the direction of IoT regulation and suggesting ways of its change. The emerging insights should help policymakers, academics, and professionals in the creation of consistent, futuristic-oriented IoT regulations that balance between innovations and privacy, trust, and accountability.

References

1. Ashton K. That ‘Internet of Things’ Thing. RFID Journal, 2009.
2. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World. W.W. Norton, 2018.
3. Bygrave LA. Data Privacy Law: An International Perspective. Oxford Univ. Press, 2014.
4. Clarke R. Information Privacy in the Digital Age. Comm. ACM,2016:10:19.
5. Ryan M. Privacy and the Internet of Things: Challenges & Opportunities. Computer L. Rev. Int’l,2020:54:1.
6. Chatterjee S, Dutta A. India’s Data Protection Law and Digital Governance. NLSIR,2022:28:45.
7. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA L. Rev.,2010:57:1701.
8. Swire P, Lagos Y. Why the U.S. Needs a Federal Privacy Law. Geo. Wash. L. Rev.,2019:77:1.
9. Information Technology Act, No. 21 of 2000. India Code, 2000.
10. Digital Personal Data Protection Act, No. 22 of 2023. India Code, 2023.
11. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
12. Telecom Regulatory Authority of India. National Telecom Machine-to-Machine (M2M) Roadmap, 2017.
13. Ministry of Housing and Urban Affairs, Government of India. Smart Cities Mission Guidelines, 2015.
14. Ministry of Health & Family Welfare. Telemedicine Practice Guidelines, 2020.
15. Federal Trade Commission Act of 1914 § 5. 15 U.S.C. § 45.
16. Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191. 110 Stat.,1996:110:1936.
17. Children’s Online Privacy Protection Act (COPPA). 15 U.S.C. §§ 6501–06, 1998.
18. Fair Credit Reporting Act (FCRA). 15 U.S.C. §§ 1681–1681x.
19. Gramm–Leach–Bliley Act (GLBA). 15 U.S.C. §§ 6801–6809.
20. California Consumer Privacy Act (CCPA). Cal. Civ. Code §§ 1798.100–1798.199, 2018.
21. California IoT Security Law. Cal. Civ. Code §§ 1798.91.04–.06, 2020.
22. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. ISO, 2022.
23. ISO/IEC 27701:2019. Privacy Information Management. ISO, 2019.
24. NIST. Security and Privacy Controls for IoT Devices (NISTIR 8259), 2020.
25. NIST. Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1), 2018.
26. Cisco. Annual Internet Report: IoT Device Growth and Trends, 2020.
27. McKinsey Global Institute. Unlocking the Potential of the Internet of Things, 2015.
28. World Economic Forum. State of IoT Security 2023.
29. OECD. Data Protection and Data Privacy in the Digital Age, 2021.
30. Internet Society. Global IoT Security Report, 2022.
31. Justice K.S. Puttaswamy (Retd.) v. Union of India. SCC,2017:10:1 (India).
32. Carpenter v. United States. S. Ct.,2018:138:2206.