# THE INTERNET OF THINGS AND FUTURE OF PRIVACY: HUMAN RIGHTS AND DISPUTE RESOLUTION APPROACH

Nitin Kumar & Pallavi Agnihotri, Lovely Professional University

**ABSTRACT**

The Internet of Things has brought humankind to a new stage when the objects cease to be inanimate devices but become the actors in our life. They monitor, document, interpret, and even foresee the behaviour of human beings. This has transformed to provide unprecedented convenience and efficiency. It has also posed some deep questions on the limits of privacy, the individual dignity and the process by which conflicts arising in this technological landscape need to be settled. This chapter examines how human rights are evolving in the world where technology studies human habits and interferes with individual choices. It analyzes the threats the Internet of Things presents to constitutional rights in India and presents a doctrinally plentiful and human rights centric framework of interpreting the future of privacy and dispute resolution.

## Introduction to a hyperconnected World

The emergence of the Internet of Things is one of the most important technological revolutions in the twenty first century. In previous decades, technology needed to be interacted upon consciously by human beings. Persons used to type commands to computers or press the screens to perform particular functions. Internet of Things has altered this basic relationship. Computer equipment is starting to talk to each other without human intervention. They feel physical surroundings, gathers behavioural data and routes them to networks that are running.

The implication of this development on human rights is immense. Once devices get to know human behaviour the boundaries between the private and the public life start fading away. The classical legal understanding of privacy was established on the assumption that human beings could make a conscious decision as to whether to release information or not. The disclosure is automatic and silent in the world of the Internet of Things. This change provokes a strong desire to gain a better insight into the possibility of preserving human dignity and individual agency.

## The IoT Data and the Change of Privacy.

Internet of Things leads to the formation of several layers of data with varying degrees of sensitivity. On the surface, there exists volunteered data, about which individuals are aware, but which they voluntarily provide when using a device. Under this we have observed data that is gathered without conscious involvement. On a more profound level is derived data that is generated out of pattern and correlations. Inferred data is the most sensitive category that predicts tendencies of behaviour and personal traits.

Improved data can help show very personal information. The anxiety can be detected by a smart watch. A smart fridge will give information on dietary habits. A smart energy meter will be able to know when there are people in a house or not. A car that is connected can observe the driving behaviour to conclude on stress or fatigue. Such patterns give an insight into what might not be clearly known by people. They create a digital identity which is not under the control of the user. The difficulty will be due to the fact that this identity will play a role in decisions that will influence the individual. Premiums may be set according to the predictions of behaviour by the insurance companies. Prospective employees can be evaluated by the employer based on the information obtained of their personal devices. The governments can utilize predictive policing technologies that utilize IoT infrastructures in the open areas. These advances render the

atmosphere where the concept of privacy is not only meant to be informational secrecy, but to be a right that safeguards autonomy, identity and personal liberty.

**Privacy and its Foundations in the Constitution.**

The Indian constitutional framework gives a good philosophical and doctrinal backing to safeguarding the privacy. Privacy was identified in the landmark decision of Justice K. S. Puttaswamy as an inherent right to life and personal liberty within the right to privacy. The ruling stated that privacy safeguards three aspects, which are interrelated. The former is bodily privacy that protects the physical body against invasive technologies. The second one is informational privacy that provides human beings with the ability to regulate the spread of personal information. The third one is decisional autonomy that guarantees the autonomy to choose without interference by coercive force or manipulation.

The dimensions are especially applicable when it comes to the Internet of Things. The technologies that track health indicators or record biometric data lead to the issue of bodily integrity. The storage systems of location or behavioural patterns are a challenge to the informational privacy. Decision making algorithms that are used to make decisions based on predictive models present dangers to the autonomy of decisions. Another important doctrine that emerged as a result of the Puttaswamy judgment was the doctrine of proportionality that required any invasion into privacy to pass a necessary test. This test dictates that any restriction on privacy should have a legitimate purpose, be essential in the fulfilment of said purpose and within its effect on rights is also reasonable.

**IoT and the Surveillance Capacity Growth.**

The Internet of Things expands the sphere and depth of surveillance along with which it was impossible to imagine even in previous decades. Surveillance is not on limited cases on the conventional cameras found in the open areas. It has since been integrated with networks of sensors which will monitor movement, communications between devices, biometric identifiers and environmental variations. These systems are often combined into smart city initiatives to provide coherent platforms of observing urban behaviour.

These systems are able to enhance services to the people. They will be able to control the traffic movement and identify accidents and optimize energy distribution. Nevertheless, they also

construct extensive behavioural collections of complete populations. In the event that the information of two or more sources is integrated, one can recreate the life of individual people with appalling precision. Such an increase in the power of surveillance presents a human rights issue since it is bound to disrupt the equilibrium of power between the person and the state. There is also increased private surveillance. Home appliances are voice-responsive. The presence of security cameras outside the homes monitors the movements of strangers and neighbours. Wearable devices are used by employers to monitor the productivity of employees. The cumulative impact of such practices is that the constant observation is normalised. This puts mental strain on the people that can inhibit the freedom of speech and undermine civic activism.

**Human rights Implications of IoT**

The IoT addresses some of the fundamental human rights. The most visible right is that of privacy. In the case of constant data recording on devices, people lose the control of when and how the information will be disclosed. Privacy does not consist of simple ability to conceal information. It is the power to control subjectivity of identity and to establish the zones of individual privacy. This is a fundamental human experience that is undermined by constant data extraction. One more important issue is connected with human dignity. When technology also defines the behaviour of the individuals in a way that they are unable to comprehend and contradict it, human dignity is at stake. The technological systems of emotional recognition and behavioural scoring systems enter the inner world of the individual. The intrusions of this kind have an influence on mental integrity which is an essential element of dignity.

The right to equality is also involved since the algorithmic systems have an ability to copy the social biases. Predictive policing systems can be at a disadvantage to marginalised groups. Recruitment algorithms can bias people who mirror the data trends of historically advantaged population groups. These results are against the principle of substantive equality that is included in Article 14 of the Indian Constitution. When people are aware that their actions are being surveilled, this is a silent condition that can and often defies the freedom of expression and association. Individuals can simply avoid going to certain sites or engaging in some form of discussion as they fear that their activities will be monitored and analyzed. This terrorism has a chilling effect that makes democratic participation weak.

**The IoT Dispute Resolution Dilemma.**

The old dispute resolution mechanisms were developed to address conflicts which occur in defined situations. They presume that the harm is visible, causation is traceable and that evidence may be judged by human judges. IT confronts these suppositions.

Most of the damages that are created by IoT systems are not visible to the victim person. An individual might never realize that there is an algorithm that refuses to give him or her a loan. They might not know that their wearable device shared their health patterns with a third party. They might not know that a smart device failed, which resulted in a security breach. Technological systems are opaque and thus hard to establish the parties that are held responsible.

There are further complications created by cross border data flow. An IoT device can be able to gather information in one country, store it in a second and process it in a third country. The issues of applicable law and jurisdiction are questioned when a dispute is at hand. The conventional legal systems are ill fitted to deal with these complexities. The large scale of the IoT implementation also brings structural issues. The amount of micro harms is uncountable with billions of devices. Individually, every harm can be minor but when combined they impact on society on a systemic scale. The number of disputes that can be presented before the court is beyond manageable. New institutional models of resolution that will combine technological skills and legal power must be developed.

**Rediscovering Dispute Resolution in IoT Systems**

An IoT-aware future oriented model of dispute resolution cannot ignore the distinctive character of harms that are associated with the Internet of Things. Creation of specialised tribunals with technical expertise in data science, cybersecurity and algorithmic accountability is one of the key aspects of such a model. Such authorities can settle the conflicts that may arise in relation to the data confidentiality or algorithmic discrimination and malfunctioning machinery. They are able to create a set of consistent standards and encourage adherence. The other factor is the necessity of explainability of algorithms. People should be given the privilege to know how they were made on decisions that affect them. This incorporates the profile of data, inference models and logic of automated processes. There should be human checks and balances to go over disputed decisions. Lack of this transparency means that the dispute

resolution process cannot be fair.

The operation of technology should incur the privacy by design principles. This implies that systems are supposed to gather the least number of data needed and keep it as little as possible. The architecture of the devices should be built with encryption and the use of secure processing methods. In instances where privacy is put as one of the values of designing systems, conflicts will automatically decrease.

Another important part can be played by online dispute resolution platforms. They are able to offer convenient, inexpensive and effective ways of settling petty conflicts that occur in the online world. These platforms may include automated assistance systems, digital mediation systems and hybrid decision making systems. This method is especially appropriate to the nature of the IoT related conflicts which have high volumes.

**IoT Governance Comparative Approaches**

Global regulatory systems provide a good understanding of how privacy and dispute resolution can be enhanced in the IoT system. The principles of data minimisation, purpose limitation and explicit consent offer very good protection to data subjects outlined in the European Union General Data Protection Regulation. It also acknowledges the right of explanation and offers formidable enforcement methods.

The California Consumer Privacy Act will enable people to choose not to sell their data and require companies to disclose the application of personal information. The characteristics enable the consumers to oppose the infringement of privacy.

The OECD principles of artificial intelligence are based on the principles of fairness, accountability and respect to human rights. They promote the application of human right impact assessment prior to the implementation of high risk technologies.

India is able to use these foreign examples and tailor their ideals to the constitutional vision and socio economic conditions. This strategy can enhance the current data protection regime and overcome the distinct pressures presented by the IoT systems.

**The Indian Regulatory Environment**

The data governance system in India has changed in the recent years substantially. Digital

Personal Data Protection Act tries to control the use and acquisition of personal information. The Act provides guidelines of consent and puts data fiduciaries under obligation. Nevertheless, the Internet of Things has some issues which the Act does not foresee fully.

The consent based models are not effective in cases where devices are gathering data in a quiet manner. Users cannot possibly give any meaningful consent whenever a device communicates with the environment. The mass surveillance by the government is also given extensive exceptions in the Act that raises some concerns regarding unregulated surveillance using IoT infrastructure.

The Act fails to provide an adequate coverage on the rights of individuals regarding inferred data and behavioural profiling. It is also not imposing very strong claims in the cases of algorithmic transparency or independent audits. These loopholes illustrate the necessity to have a more detailed IoT specific framework. Health and telecommunications/consumer protection Sectoral regulation occasionally overlaps, and occasionally transpires as a regulatory void. People and technology providers are left in the dark because of the absence of a single solution.

**Doctrinal and Policy Recommendations**

The Internet of Things should have a strong legal framework, which should start by considering the establishment of mental privacy as a fundamental element of human dignity. Emotion or cognition-monitoring technologies are hazardous to a degree that exceeds the conventional privacy concept. It ought to create a constitutional doctrine of cognitive liberty that safeguards inner mental world of people.

Algorithms fairness must be considered as a legal requirement. The developers and companies must be made to complete bias tests with representative datasets. Lack of ensuring fairness should call forth liability. Data protection authorities that are independent should be given the powers of investigation, rule making and the power to issue a penalty. These are powers that cannot be influenced by politics.

The IoT governance should involve the community. The transparent policies applied to the operation of the IoT devices in the public spaces must include the views of the citizens. Accountability can be developed by the formation of local data stewardship councils. In the management of cross border data flows international cooperation is necessary. India must strive

to have treaties that integrate privacy protection, facilitate secure transfer of data and create international dispute resolution mechanism.

## Conclusion

The Internet of Things has established a virtual world where the human activity and experiences are constantly converted into information. This is a convenient and innovative setting that also subjects people to previously unseen dangers. Privacy ceases being a passive privilege that guarantees confidentiality. It has become a proactive right that preserves autonomy, dignity and is able to make meaningful choices in life. The Indian legal system has constitutional principles that have a sound ethical ground when protecting these rights. Nevertheless, the high pace of the development of IoT technologies demands the same speed of the revision of the legal doctrine and dispute resolution practices. Human rights in a globalized world could be seen in the future as they are able to integrate dignity, fairness and accountability in the technology platforms that determine day to day life.

Rights centred IoT governance model does not just represent a regulatory requirement. It is an ethical command that acknowledges the worth of the human person at the time of smart computers looking at the world and making sense. To ensure the safety of people in this world, one has to exercise vigilance, be innovative and re-committed to justice. It is the quest of human freedom itself to gain the privacy and dignity in the digital age.

**BIBLIOGRAPHY:**

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

**Annotation:** *This Supreme Court judgement is the foundational text for the right to privacy in India. It conceptualises privacy as part of the right to life and personal liberty and introduces the proportionality test for determining valid State intrusion. The chapter relies heavily on this decision to establish the constitutional basis for privacy in the context of the Internet of Things and to explain how modern technologies interact with bodily, informational and decisional privacy.*

**2. Digital Personal Data Protection Act, 2023 (India)**

**Annotation:** *The DPDP Act forms the primary statutory framework governing personal data in India. It provides definitions, obligations for data fiduciaries, and rights for data principals. The Act is used to highlight gaps in regulating IoT systems, particularly in areas such as inferred data, algorithmic profiling, cross-border data flow, and consent fatigue. It forms the legislative backdrop for the chapter's policy recommendations.*

**3. General Data Protection Regulation (GDPR), European Union, 2018**

**Annotation:** *The GDPR is widely regarded as the strongest data protection regime globally. It introduces key concepts like data minimisation, purpose limitation, explicit consent, and the right to explanation for automated decisions. This source is used to compare India's data governance landscape with international standards and to demonstrate best practices for regulating IoT technologies in a human-rights-oriented framework.*

**4. Solove, Daniel J. Understanding Privacy. Harvard University Press, 2008.**

**Annotation:** *Solove's work is crucial for understanding the conceptual nature of privacy. He develops a taxonomy that includes information collection, processing, dissemination, and invasion. The chapter draws on Solove to explain how IoT systems disrupt traditional privacy models and why existing legal frameworks struggle to deal with behavioural profiling and passive data generation.*

**5. Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.**

**Annotation:** *Zuboff offers a detailed examination of how digital corporations extract and monetise behavioural data. Her insights are used to explain how IoT ecosystems feed into surveillance capitalism and how this affects autonomy, dignity, and freedom of choice. The chapter employs her analysis to build arguments around algorithmic power imbalances and human rights risks.*

**6. OECD. "OECD Principles on Artificial Intelligence." Organisation for Economic Co-operation and Development, 2019.**

**Annotation:** *The OECD principles emphasise transparency, accountability, safety, and respect for human rights in AI development. These guidelines support the chapter's recommendations for algorithmic fairness, impact assessments, and rights-by-design approaches. This source provides an international normative framework for regulating IoT and automated decision systems.*

**7. Schwab, Klaus. The Fourth Industrial Revolution. World Economic Forum, 2016.**

**Annotation***: Schwab's text describes the convergence of digital, biological, and physical systems, including IoT. It helps contextualise how IoT reshapes social structures, governance, and human interactions. The chapter uses this source to discuss the transformative nature of IoT technologies and their implications for human rights and dispute resolution mechanisms.*

**8. Hildebrandt, Mireille. Smart Technologies and the End(s) of Law. Edward Elgar Publishing, 2015.**

**Annotation:** *Hildebrandt examines how smart systems challenge legal institutions by creating environments of data-driven decision making. Her analysis helps the chapter articulate why traditional dispute resolution is insufficient in IoT contexts and how algorithmic transparency and new institutional mechanisms must evolve to maintain the rule of law.*

**9. DeNardis, Laura. The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press, 2020.**

**Annotation:** *DeNardis explores the political and social consequences of IoT infrastructure.*

*Her work illustrates how objects embedded with network connectivity influence public governance, surveillance practices, and personal freedoms. The chapter uses this to develop arguments about State power, public-space IoT systems, and the expansion of surveillance capacity.*

**10. Calo, Ryan. "Privacy Harm." Georgia Law Review, vol. 48, no. 3, 2014, pp. 733–800.**

**Annotation:** *Ryan Calo introduces the concept of privacy harms, distinguishing between subjective and objective harms such as manipulation, emotional intrusion, and exploitation. His framework helps the chapter analyse how IoT technologies create psychological and behavioural harms that traditional legal doctrines struggle to capture. This supports the human-centred approach of the chapter.*