Int J Ethics Soc 2026; 7(4): 12-21

10.22034/ijethics.7.4.425

INTERNATIONAL JOURNAL OF Ethics & Society

Review Article

Data Ethics and Privacy in the Age of the Internet of Things: Risks and Responsibilities of Social Trust

Charith Perera[1*], Rajiv Ranjan[2], Lizhe Wang[3], Samee U. Khan[4], Albert Y. Zomaya[5]

1. School of Computer Science and Informatics, Cardiff University, UK.
2. School of Computing, Newcastle University, Newcastle, UK.
3. School of Computer Science, University of Geoscience, China.
4. Department of Electrical and Computer Engineering, Mississippi State University Starkville, USA.
5. Centre for Distributed and High Performance Computing, School of Computer Science, University of Sydney, Australia.

Corresponding Author: Charith Perera, School of Computer Science and Informatics, Cardiff University, UK. E-mail: charith.perera@acm.org

Received 10 Sep 2025 **Accepted** 15 Oct 2025 **Online Published** 04 Jan 2026

Abstract

Introduction: The rapid expansion of the Internet of Things (IoT) as one of the most transformative technologies of the digital age has led to the production and processing of vast volumes of personal and contextual data. While this transformation offers significant opportunities to improve quality of life, it also generates profound ethical challenges, particularly in the areas of privacy and data management. The invisible, automated, and pervasive nature of data collection within the IoT ecosystem calls into question traditional concepts of informed consent, individual control over data, and ethical accountability, and intensifies risks such as pervasive surveillance, data misuse, information insecurity, and the erosion of individual autonomy.
Material and Method: This article adopts a review–analytical approach to examine the scientific literature related to data ethics and privacy in the Internet of Things. Based on existing studies, it explores the foundational aspects of the topic and ultimately draws conclusions from the information reviewed.
Conclusion: The study demonstrates that privacy in this context requires a contextual and relational redefinition. The findings indicate that ethical responsibility within the IoT data cycle is distributed in nature, and that multiple actors-from designers and companies to governments-play a fundamental role in upholding principles of data ethics. Ultimately, it can be argued that adherence to data ethics and privacy principles is a prerequisite for the formation of social trust and the sustainable acceptance of the Internet of Things. Without simultaneous attention to technical, ethical, and social dimensions, the development of this technology will face serious challenges.
Keywords: *Data Ethics, Privacy, Internet of Things, Social Trust.*

How to Cite: Perera C, Ranjan R, Wang L, Khan S.U., Zomaya A.Y. Data Ethics and Privacy in the Age of the Internet of Things: Risks and Responsibilities of Social Trust, Int J Ethics Soc. 2026;7(4): 12-21. doi: 10.22034/ijethics.7.4.425

INTRODUCTION

The rapid growth of digital technologies in recent decades, particularly the emergence and expansion of the Internet of Things (IoT), has brought about a fundamental transformation in the way humans interact with their environment, technology, and data. The Internet of Things refers to a network of physical objects connected to the internet that, through sensors, software, and data processing systems, are capable of collecting, exchanging, and analyzing vast amounts of data [1]. This technology has penetrated areas such as smart healthcare, smart cities, transportation, agriculture, industry, and

Copyright © 2026 Perera C. et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License(http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

everyday life, and promises increased efficiency, improved decision-making, and enhanced quality of human life.

Despite these benefits, the large-scale production and processing of data within the IoT ecosystem have given rise to deep ethical and social challenges. Data collected by smart devices often include sensitive, personal, and contextual information about individuals' behavior, location, health status, and lifestyle patterns [2]. These characteristics have made the Internet of Things one of the most complex technological environments from the perspective of data ethics and privacy.

Data ethics, as an emerging branch of applied ethics, examines the principles, values, and norms that should govern the data life cycle-from collection and storage to analysis, sharing, and deletion [3]. In the context of the Internet of Things, data ethics gains heightened importance, as many data collection processes occur invisibly, automatically, and without users' full awareness. This situation challenges traditional notions of informed consent, individual control over data, and privacy.

Privacy in the age of the Internet of Things is no longer merely about protecting individual data in isolation; rather, it has taken on a contextual and networked character. The theory of "contextual integrity" suggests that a violation of privacy occurs when information flows exceed expected social and contextual norms. In IoT-based environments, these flows are often complex, multilayered, and transboundary, placing them beyond the control of ordinary users [4].

The ethical and social risks of the Internet of Things include privacy violations, data misuse, pervasive surveillance, algorithmic discrimination, data insecurity, and the loss of individual autonomy [5]. Moreover, weaknesses in the cybersecurity of IoT devices can lead to data breaches and pose serious threats to both individual and societal security. These risks have not only technical consequences but also profound impacts on public trust in technology.

In this context, the issue of ethical accountability among various actors-from technology designers and developers to companies, governments, and legislators-plays a key role in shaping social trust. Legal frameworks such as the European Union's General Data Protection Regulation (GDPR) have attempted to address some of these challenges by emphasizing principles such as transparency, data minimization, accountability, and users' right to control their data [6]. However, the pace of technological change often exceeds the capacity of existing laws, highlighting the necessity of ethics-centered approaches.

Social trust, as a prerequisite for the acceptance and sustainable use of the Internet of Things, emerges when users are confident that their data are managed responsibly, fairly, and securely [7]. Therefore, examining the relationship between data ethics, privacy, and social trust is essential for understanding the long-term implications of the Internet of Things.

Accordingly, the present article aims to provide a systematic analysis of the scientific literature related to data ethics and privacy in the age of the Internet of Things. By identifying key risks, it seeks to examine the ethical responsibilities of various actors and their role in shaping social trust. This review can provide a theoretical foundation for future research and for ethics-oriented policymaking in the field of smart technologies.

MATERIAL AND METHODS

This article adopts a review–analytical approach to examine the scientific literature related to data ethics and privacy in the Internet of Things. Based on existing studies, it explores the foundational aspects of the topic and ultimately draws conclusions from the information reviewed.

DISCUSSION

Ethical Privacy Risks in the Internet of Things Ecosystem

Due to its pervasive, automated, and data-driven nature, the Internet of Things ecosystem provides a setting for the emergence of a range of complex ethical risks in the domain of privacy that go beyond the well-known challenges of traditional digital technologies. Unlike systems based on direct user interaction, many IoT devices collect data invisibly and continuously, data that are often highly personal, contextual, and sensitive [1]. This characteristic significantly disrupts the balance of power between users and data controllers and raises fundamental questions about the ethical legitimacy of data collection and use.

One of the most significant ethical risks is the weakening of the concept of informed consent. In IoT environments, users are often not fully aware of the types of data being collected, the purposes of processing, or the stakeholders who have access to the data. As a result, consent-one of the core pillars of data ethics and data protection regulations-is reduced to a formalistic and ineffective concept [3]. Research indicates that the complexity of the IoT ecosystem effectively deprives users of the possibility of making informed choices and exposes them to a form of "technological coercion" [8].

Another major ethical risk concerns data accumulation and linkability. Seemingly non-sensitive data collected by various IoT devices can, when combined, generate detailed patterns of individuals' behavior, preferences, health status, and even beliefs. This capacity for secondary re-identification weakens the boundary between personal and non-personal data and constitutes a serious threat to both individual and collective privacy [5]. From an ethical perspective, such processes may lead to violations of the principles of proportionality and data minimization.

Moreover, the Internet of Things enables the formation of pervasive and continuous surveillance. Smart home devices, wearables, and urban infrastructures can create a form of constant monitoring that often occurs without effective user control. This situation, particularly within the framework of surveillance capitalism, can result in the gradual erosion of individual autonomy and the normalization of privacy violations [8]. Such dynamics become especially problematic when information flows exceed socially accepted contextual norms.

Security risks also play a significant role in intensifying ethical privacy challenges. Widespread weaknesses in the security design of many IoT devices increase the likelihood of data breaches, unauthorized access, and misuse of personal information. This issue is not merely a technical challenge; from an ethical standpoint, it reflects a failure to uphold the duty of care toward users [7].

Ultimately, these risks have consequences that extend beyond the individual level and can lead to a decline in social trust in smart technologies. When users feel that they lack control over their data or that their information is vulnerable to misuse, their willingness to adopt and use the Internet of Things diminishes. Therefore, ethical privacy risks represent not only a threat to individual rights but also a barrier to the sustainable and responsible development of the Internet of Things.

Redefining Privacy in the Age of the Internet of Things

The expansion of the Internet of Things has challenged the traditional concept of privacy, which was largely based on individual control over personal information and clearly defined boundaries between private and public spheres. In the IoT ecosystem, data are collected continuously, automatically, and often without direct user interaction, highlighting the need for

theoretical reconsideration of the definition of privacy [9]. From this perspective, privacy is no longer merely a static individual right, but a dynamic, contextual, and networked phenomenon.

One of the most influential approaches to redefining privacy is the theory of contextual integrity proposed by Nissenbaum. According to this view, a violation of privacy occurs not simply due to the disclosure of information, but when information flows exceed the social norms governing a specific context [10]. In IoT-based environments, where data are transferred among multiple actors and across diverse contexts, maintaining such integrity has become increasingly difficult. Consequently, an exclusive focus on individual consent cannot, by itself, guarantee effective privacy protection.

Furthermore, the Internet of Things highlights the concept of collective privacy. Data generated by an individual, particularly in shared spaces such as smart homes or smart cities, can also reveal information about other individuals or groups. This demonstrates that privacy in the age of the Internet of Things is not limited to individual decisions and requires a social and collective understanding [3]. From the perspective of data ethics, this situation necessitates the development of frameworks that also take potential benefits and harms at the societal level into account.

In addition, the integration of the Internet of Things with advanced data analytics has weakened the boundary between personal and non-personal data. Seemingly trivial data, when combined with other data sources, can lead to the re-identification of individuals and the prediction of their behavior [5]. Therefore, definitions of privacy must move beyond an exclusive focus on data type and instead consider inferential capabilities and the consequences of data use.

From legal and ethical perspectives, these developments indicate that traditional approaches based on notice and consent are insufficient for effectively protecting privacy in the IoT ecosystem. Scholars have emphasized the need to shift toward approaches such as Privacy by Design and ethics by design, in which ethical principles are incorporated from the earliest stages of technological development [7, 11]. Such approaches regard privacy not as an obstacle, but as a foundational element in the design of smart technologies.

Overall, redefining privacy in the age of the Internet of Things requires a multidimensional perspective that simultaneously considers individual, collective, contextual, and technological dimensions. This redefinition is an unavoidable necessity not only for protecting users' rights, but also for strengthening social trust and ensuring the sustainable adoption of the Internet of Things.

Ethical Responsibility of Different Actors in the IoT Data Cycle

One of the fundamental challenges of data ethics in the Internet of Things ecosystem is the identification and distribution of ethical responsibility among the multiple actors involved in the data life cycle. Unlike traditional systems, in which responsibility was often confined to a single identifiable entity or organization, in the IoT data are produced, processed, analyzed, stored, and reused within a complex, multilayered network of actors. This situation gives rise to a form of "distributed responsibility," in which ethical accountability cannot be easily attributed to a single actor [7].

The IoT data cycle typically includes the stages of data collection, transmission, storage, analysis, sharing, and secondary use. At each of these stages, different actors-from hardware and software designers to platform companies, governmental bodies, and end users-play a role. From the perspective of data ethics, each of these actors bears specific obligations to protect

privacy, ensure fairness, promote transparency, and maintain social trust [3].

- Ethical responsibility of technology designers and developers: The first level of ethical responsibility lies with the designers, engineers, and developers of IoT systems. Decisions made during the technical design stages-such as the types of data collected, the level of data granularity, default data-sharing settings, and security architectures-have a direct impact on the extent to which privacy is either violated or protected. Accordingly, approaches such as Ethics by Design and Privacy by Design have been proposed as key normative principles [12]. Under these approaches, developers are required to consider ethical concerns not as an add-on, but as an integral part of system design. Ignoring the ethical implications of technical decisions, even in the absence of malicious intent, can lead to ethical responsibility, as designers are in a position to foresee and mitigate potential risks [5].
- Ethical responsibility of companies and platform providers: Companies and organizations that collect and process IoT data are at the center of ethical disputes concerning privacy. These actors typically possess significant informational and power asymmetries vis-à-vis users and are able to exploit data for commercial purposes, behavioral prediction, or targeted advertising [8]. From an ethical standpoint, such power entails a higher level of accountability. The ethical responsibilities of companies include transparency in data policies, limiting secondary data use, ensuring data security, and respecting users' autonomy. Research indicates that even within legal frameworks such as the GDPR, mere minimal compliance with legal requirements does not necessarily constitute ethical behavior, and companies are expected to go beyond legal obligations [3].
- Ethical responsibility of governments and regulatory bodies: Governments and policymakers play a crucial role in shaping the ethical environment of the Internet of Things. On the one hand, they are responsible for protecting citizens' rights against data misuse through legislation and standards; on the other hand, they themselves are major consumers of IoT data in areas such as smart cities, healthcare, and public security. From an ethical perspective, governments must strike a balance between technological innovation and privacy protection. An exclusive focus on efficiency and security may serve to justify extensive surveillance and the erosion of citizens' fundamental rights [4]. Therefore, the ethical responsibility of governments extends beyond lawmaking to include the creation of institutional trust and the assurance of the social legitimacy of data use.
- Ethical responsibility of users and its limitations: Although users also act as data producers, attributing heavy ethical responsibility to them is controversial. In the IoT ecosystem, users often interact with systems whose technical complexity, lack of transparency, and restrictive default designs significantly limit the possibility of informed choice. Consequently, an excessive emphasis on "individual user responsibility" may result in an unjust transfer of responsibility from powerful actors to individuals [13].
- Distributed ethical responsibility and its implications for social trust: Overall, ethical responsibility in the IoT data cycle is networked and distributed in nature. This condition can lead to a phenomenon known as "moral overload," in which no single actor is capable of fully ethical action on their own [7]. If not properly managed, this situation can erode social trust and provoke user resistance to smart technologies.

Therefore, strengthening social trust requires clarifying responsibilities, fostering cooperation among stakeholders, and embracing the principle that data ethics in the Internet of Things is not an individual duty, but a collective and institutional commitment.

Data Ethics and the Formation or Erosion of Social Trust

Social trust is a key component in the acceptance, sustainable use, and legitimacy of emerging technologies, particularly the Internet of Things. In the IoT ecosystem-characterized by the continuous collection, processing, and analysis of large-scale and often sensitive data-data ethics plays a decisive role in either building or undermining this trust. Studies indicate that users' trust in technology depends not only on technical performance, but also on how data are managed, the extent to which ethical principles are respected, and the level of accountability among involved actors [7].

From a theoretical perspective, social trust emerges when users believe that their data are used fairly, transparently, securely, and in proportion to the stated purposes [2, 14]. By emphasizing principles such as transparency, informed consent, data minimization, accountability, and respect for individual autonomy, data ethics provides a normative framework for fostering such beliefs. In the absence of these principles, the Internet of Things may become a source of distrust and social resistance rather than a platform for social empowerment.

One of the primary factors contributing to the erosion of social trust in the Internet of Things is the lack of transparency throughout the data cycle. Users often do not know what data are collected, when, by which devices, and for what purposes they are processed. This ambiguity, particularly when combined with business models based on data extraction and commercialization, intensifies feelings of loss of control and undermines trust [8]. From the perspective of data ethics, such conditions conflict with the principle of respect for persons and the right to know.

In addition, repeated privacy violations and data breaches in IoT systems have a direct impact on public attitudes toward technology. Research shows that experiencing, or even merely being aware of, a data breach can reduce users' trust not only in a specific product or company, but in the entire technological ecosystem [15]. This demonstrates that social trust is a fragile and cumulative phenomenon, and that the ethical negligence of a single actor can have consequences that extend beyond the individual level.

From a social perspective, data ethics is also closely linked to issues of justice and equality. Unethical uses of IoT data can lead to algorithmic discrimination, social exclusion, and the reproduction of structural inequalities. Such outcomes, particularly in domains such as smart cities, digital health, and urban surveillance, weaken the trust of different social groups in technological and governmental institutions [16]. Conversely, the design and implementation of ethics-oriented data policies can strengthen perceptions of fairness and social legitimacy.

Another important point is that social trust in the Internet of Things does not arise solely from user–technology interactions, but is the product of institutional relationships and data governance. Regulatory frameworks such as the GDPR, by emphasizing user rights and organizational accountability, have sought to strengthen public trust through the institutionalization of data ethics [6]. However, the literature suggests that laws alone are insufficient, and that without genuine ethical commitment at the levels of design and implementation, sustainable social trust will not be achieved [2].

In conclusion, data ethics in the Internet of Things ecosystem plays a dual role: on the one hand, neglect of ethical principles can lead to the erosion of social trust, user resistance, and a crisis of technological legitimacy; on the other hand, the institutionalization of data ethics can function as an enabling factor that facilitates social acceptance, informed user participation, and the responsible development of the Internet of Things. Accordingly, social trust should be regarded not as a secondary byproduct, but as a fundamental indicator for evaluating the ethical success of data-driven technologies.

Theoretical, Practical, and Policy Implications

The findings derived from the literature review on data ethics and privacy in the Internet of Things carry significant implications at the theoretical, practical, and policy levels. The complexity of the IoT ecosystem-in which data are continuously, invisibly, and at large scale produced and processed-indicates that addressing the ethical challenges of this domain requires a rethinking of existing conceptual frameworks and the adoption of multi-level approaches [3].

From a theoretical perspective, the literature suggests that classical concepts of privacy and data ethics are insufficient to explain the realities of the Internet of Things. In many traditional theories, privacy is primarily defined as an individual right based on personal control over data. However, within the IoT ecosystem, data are often generated in collective, contextual, and networked forms, and their consequences extend beyond any single individual [4]. This highlights the need to develop approaches such as contextual privacy, collective privacy, and information ethics.

Moreover, the findings point to the necessity of integrating theories of technology ethics with theories of social trust. Trust is no longer merely the outcome of proper technological functioning, but rather the product of interactions among ethical values, institutional transparency, and users' perceptions of fairness and accountability [7]. Accordingly, the development of interdisciplinary theoretical frameworks that connect data ethics, science and technology studies, and social theories of trust represents one of the most important theoretical implications in this field.

At the practical level, the results of this review indicate that organizations and technology developers must regard data ethics as an inseparable part of the design and implementation of IoT systems. Approaches such as Privacy by Design and Ethics by Design can help reduce ethical risks and enhance user trust [9]. This requires that ethical considerations be incorporated not at the final stages, but from the very beginning of the data and system life cycle.

Transparency in the collection, processing, and sharing of data also plays a critical role in strengthening social trust. Studies show that users are more willing to accept smart technologies when they can understand the logic of system decision-making and the fate of their data [5]. Therefore, the development of explainability tools, comprehensible user interfaces, and effective mechanisms that enable users to exercise control over their data constitutes one of the most important practical implications for actors in the IoT industry.

At the policy level, the reviewed literature indicates that existing legal frameworks, while an important step toward data protection, are not sufficient on their own to address the ethical complexities of the Internet of Things. Regulations such as the GDPR, by emphasizing principles such as transparency, accountability, and data minimization, have provided an important foundation for privacy protection [6], yet the pace of technological change and the transboundary nature of IoT data have created new challenges.

Accordingly, policymaking in the IoT domain should move toward anticipatory, flexible, and ethics-oriented approaches. The participation of diverse stakeholders-including governments, industry, civil society, and users-in the policy development process can enhance legitimacy and effectiveness [3]. Furthermore, attention to cultural and social differences in the understanding of privacy and trust is essential to avoid the imposition of uniform and ineffective models at the global level.

Overall, the theoretical, practical, and policy implications derived from this review demonstrate that responsibly addressing the challenges of data ethics and privacy in the Internet of Things requires a holistic perspective that simultaneously considers theoretical foundations, practical requirements, and regulatory mechanisms. Such an approach can facilitate the development of trustworthy smart technologies aligned with human values in the digital age.

Critical Considerations of the Topic

The scientific literature on data ethics and privacy in the Internet of Things reflects a growing consensus on the importance of these challenges; however, a critical examination of this body of research reveals that many existing approaches remain reactive, technology-centered, and individualistic. A substantial portion of studies conceptualize privacy risks primarily as technical or legal issues and focus on solutions such as improving security, encryption, or regulatory compliance [1, 6]. While necessary, this focus appears insufficient to address the deeper social and ethical consequences of the Internet of Things.

One of the fundamental shortcomings of the existing literature is the persistence of a traditional understanding of privacy. Many frameworks continue to define privacy as an individual right based on informed consent and personal control over data, even though in the IoT ecosystem such control is often illusory. The automated, continuous, and invisible collection of data deprives users of meaningful choice and reduces consent to a merely formal mechanism [3]. From this perspective, it can be argued that insistence on individual-centered models contributes to the reproduction of power asymmetries between users and dominant technological actors.

Furthermore, data ethics literature on IoT often neglects the collective and structural dimensions of privacy. As scholars emphasize, privacy violations do not occur solely at the individual level, but can alter the informational norms of entire social contexts [4, 17]. In the Internet of Things, data generated by one individual may have implications for family members, neighbors, or even broader social groups. Nevertheless, many existing ethical and legal frameworks are not yet adequately prepared to address the concept of "collective privacy."

From the perspective of ethical responsibility, although the notion of distributed accountability has gained attention in recent years, in practice responsibilities are often unevenly allocated among actors. Users, as the weakest link in the chain, bear the main burden of risks, while technology companies and platforms possess greater structural and economic power [7, 18]. This imbalance raises serious questions about ethical and social justice in the data-driven economy of the Internet of Things.

The discussion of social trust in the existing literature is also sometimes framed in an instrumental and functional manner, treating trust merely as a factor for increasing technology adoption and market growth [19]. Such an approach risks transforming trust from an ethical value into a tool for legitimizing problematic practices of data collection and exploitation [2]. From a critical standpoint, social trust can only be sustainable and meaningful when it is grounded

in genuine transparency, institutional accountability, and respect for human autonomy, rather than being engineered through persuasive designs or minimal disclosure policies.

Overall, this critical examination demonstrates that the ethical challenges of data ethics and privacy in the Internet of Things cannot be resolved merely by adding layers of regulation or protective technologies. What is required is a profound rethinking of theoretical assumptions, power distributions, and the values that govern the design and governance of data. Without such reconsideration, there is a risk that the Internet of Things, instead of serving as a tool to enhance quality of life, will become a mechanism for intensifying surveillance, inequality, and the erosion of social trust.

CONCLUSION

This review article sought to elucidate the ethical dimensions of data and privacy in the context of the Internet of Things and to examine their implications for social trust. It demonstrated that the Internet of Things is not merely a technological transformation, but a deeply social, ethical, and political phenomenon that has redefined traditional boundaries between data, technology, and everyday human life. The findings of the literature review indicate that the inherent characteristics of the IoT ecosystem-including pervasiveness, automation, the invisibility of data collection, and data linkability-have generated unprecedented ethical risks in the domain of privacy that cannot be fully managed through classical conceptual and legal frameworks.

The results show that privacy in the age of the Internet of Things can no longer be defined solely as an individual right over personal data, but must be reconsidered as a contextual, relational, and collective phenomenon. Data flows in IoT environments often occur beyond users' awareness and control, fundamentally challenging concepts such as informed consent and free choice. Under such conditions, privacy violations may become not exceptional events, but structural and normalized states.

From a data ethics perspective, the article demonstrates that responsibility for privacy protection and fair data use in the IoT ecosystem is distributed and multi-level. Technology designers and developers, companies and platforms, governments and regulators, and even users each play distinct yet interrelated roles in the IoT data life cycle. However, excessive emphasis on user responsibility, without attention to asymmetries in power, knowledge, and control, can lead to a form of "unjust transfer of ethical responsibility." Consequently, ethics-oriented approaches such as Ethics by Design and Privacy by Design play a crucial role in mitigating risks and strengthening accountability.

One of the most significant findings of this article is the deep connection between data ethics and social trust. Users' and society's trust in the Internet of Things depends not only on its technical efficiency, but also on perceptions of fairness, transparency, accountability, and respect for human rights. Recurrent privacy violations, opacity in algorithmic functioning, and commercial or surveillance-oriented misuse of data can erode social trust and, in turn, reduce the social acceptance and legitimacy of the Internet of Things. Conversely, ethical data governance can function as a form of social capital that enables the sustainable and responsible use of this technology.

In terms of theoretical implications, this article emphasizes the need to develop interdisciplinary ethical frameworks capable of addressing the technological, social, and cultural complexities of the Internet of Things in an integrated manner. From a practical perspective, the findings indicate that reliance on legal regulation alone is insufficient, and that ethical, educational, and design-oriented mechanisms must be employed

simultaneously. At the policy level, there is an increasing need for anticipatory, participatory regulation that is sensitive to cultural and social contexts.

Overall, this article concludes that the future of the Internet of Things is closely tied to how data ethics and privacy are addressed. Without serious attention to these dimensions, the Internet of Things may become a tool for intensifying inequality, pervasive surveillance, and social distrust. By contrast, if ethical principles are treated as an integral part of the design, implementation, and governance of this technology, the Internet of Things can serve to enhance quality of life, strengthen social trust, and promote sustainable development. Achieving this vision requires the sustained commitment of all stakeholders to ethical responsibility and interdisciplinary dialogue.

ETHICAL CONSIDERATIONS

Ethical issues (such as plagiarism, conscious satisfaction, misleading, making and or forging data, publishing or sending to two places, redundancy and etc.) have been fully considered by the writers.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

FUNDING DECLARATION

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

REFERENCES

1. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks, 2010; 54(15): 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
2. Zuboff S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs. 2019.
3. Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, Luetge C, Madelin R, Pagallo U, Rossi F, Schafer B, Valcke P, Vayena E. AI4People-an ethical framework for a good ai society: opportunities, risks, principles, and recommendations. Minds and Machines, 2018; 28(4): 689–707. https://doi.org/10.1007/s11023-018-9482-5
4. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press. 2009.
5. Mittelstadt B D, Allo P, Taddeo M, Wachter S, Floridi L. The ethics of algorithms: Mapping the debate. Big Data & Society, 2016; 3(2). https://doi.org/10.1177/2053951716679679
6. European Union. General Data Protection Regulation (GDPR). Official Journal of the European Union. 2016.
7. Van den Hoven J, Lokhorst GJ, Van de Poel I. Engineering and the problem of moral overload. Science and Engineering Ethics, 2012; 18: 143–155. https://doi.org/10.1007/s11948-011-9277-z
8. Tang RW, Mi L, Chan X W C. et al. Corporate social responsibility and technological advancement of international service enterprises: links and gaps in the literature. Management International Review, 2025; 65: 415–458. https://doi.org/10.1007/s11575-025-00578-4
9. Ziegeldorf J, Morchon O, Wehrle K. Privacy in the Internet of Things: Threats and challenges. security and communication networks. 2014; 7(12). https://doi.org/10.1002/sec.795
10. Perera C, Ranjan R, Wang L, Khan S, Zomaya A. Big data privacy in the internet of things era. IT Professional. 2014; 17(3). https://doi.org/10.1109/MITP.2015.34
11. Aleisa N, Renaud K. Privacy of the internet of things: a systematic literature review (Extended Discussion). 2016. https://doi.org/10.48550/arXiv.1611.03340
12. Cavoukian A. Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era. 2011; 4: 170-208. https://doi.org/10.4018/978-1-61350-501-4.ch007
13. Solove D J. The myth of the privacy paradox. SSRN Electronic Journal. 2020; https://doi.org/10.2139/ssrn.3536265
14. van der Zeeuw A, van Deursen A J, Jansen G. Inequalities in the social use of the Internet of things: A capital and skills perspective. New Media & Society, 2019; 21(6): 1344-1361. https://doi.org/10.1177/1461444818821067
15. Patil D A. A comprehensive survey on securing the social internet of things: protocols, threat mitigation, technological integrations, tools, and performance metrics. Science Report, 2025; 15: 40190. https://doi.org/10.1038/s41598-025-23865-4
16. Malekshahi Rad M, Rahmani AM, Sahafi A. et al. Social Internet of Things: vision, challenges, and trends. Human-centric Computing and Information Sciences, 2020; **10**: 52. https://doi.org/10.1186/s13673-020-00254-6
17. Popescul D, Georgescu M. Internet of things–some ethical issues. The USV Annals of Economics and Public Administration. 2013; 13(2): 210-216.
18. Dhinakaran D, Edwin Raja S, Ramathilagam A, Vennila G, Alagulakshmi A. Ethical and legal challenges with IoT in home digital twins. MethodsX, 2025; 14: 103409. https://doi.org/10.1016/j.mex.2025.103409
19. Abdelghani W, Zayani C, Amous I, Sedes F. Trust management in social internet of things: a survey. Springer Nature Link, 2016; 9844: 430-441. https://doi.org/10.1007/978-3-319-45234-0_39