A screenshot of a computer

AI-generated content may be incorrect.

# Assessment Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assessment title Abr. Weighting**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Ethical, legal and professional issues in IT |  | WRIT1 |  | 100% |   Pass marks are 40% for undergraduate work and 50% for postgraduate work unless stated otherwise. |

|  |  |  |
| --- | --- | --- |
| **Task/assessment brief:**  Select a technology, case study, or an information system relevant to the module scope (Eg: IOT, Big Data, Privacy, social media, IP, Surveillance system etc.) and conduct research to identify the relevant ethical, social, legal and professional concerns related to the selected topic. Evaluate and discuss the issues identified covering the following tasks.    Write an essay covering the following areas related to the chosen topic.     1. Identify the issues in terms of ethical, legal professional and social concerns of the selected topic. Critically evaluate different perspectives of the issues / concerns raised by applying relevant ethical principles, Acts and professional code of conducts. **(45 Marks) (2000 Words)** **(LO1)**   **(LO2)**   1. Discuss the different perspectives, arguments raised by other writers that have researched the ethical, legal, social and professional concerns of the same technology/ topic. Use creditable sources to conduct the research **(25Marks) (1000 Words) (LO1) (LO2)** 2. Provide recommendations to mitigate the issues identified. Recommendation should be based on the creditable sources. **(15Marks) (600 Words) (LO1) (LO2)** 3. Discuss the importance of ethical approach for the chosen topic and explain how it is helping an   IT professional for his professional development. **(400 Words) (10Marks) (LO3)**   1. Correct use of citation, referencing and use of credible and authoritative sources using Harvard referencing **(5 Marks)** | | |
| **Word count (or equivalent):** | 4000 |  |

This a reflection of the effort required for the assessment. Word counts will normally include source code, any text, tables, calculations, figures, subtitles and citations. Reference lists and contents of appendices are excluded from the word count. Contents of appendices are not usually considered when determining your final assessment grade.

**Assignment Cover Sheet**

|  |  |  |
| --- | --- | --- |
| **Qualification** | | **Module Number and Title** |
| BSC in Computing & Software Engineering | | CIS6004 - Professional & Ethical Issues in IT |
| **Student Name & No.** | | **Assessor** |
| R.G Pramod Sandakelum  Registration Number GM/BSCSD/04/08  University Number ST20261236 | | Mrs. Sankani Heenkenda |
| **Hand out date** | | **Submission Date** |
| 12/01/2025 | | 09/03/2025 |
| **Assessment type**  **Assignment 1** | **Duration/Length of**  **Assessment Type**  WRIT1-Coursework: (Individual ) 4000 words equivalent | **Weighting of Assessment**  **100%** |

|  |  |
| --- | --- |
| **Learner declaration** | |
| I, R.G Pramod Sandakelum GM/BSCSD/04/08 / ST20261236, certify that the work submitted for this assignment is my own and research sources are fully acknowledged. | |
| |  |  |  |  | | --- | --- | --- | --- | | **Marks Awarded** | | | | | First assessor | |  | | | IV marks | |  | | | Agreed grade | |  | | | Signature of the assessor |  | Date |  | |

**Feedback Form**

**International College of Business & Technology**

**Module :** CIS6004 - Professional & Ethical Issues in IT

**Student :** R.GPramod Sandakelum GM/BSCSD/04/08 / ST20261236

**Assessor :** Mrs. Sankani Heenkenda

**Assignment : WRIT1-Coursework: (Individual) 4000 words equivalent**

**Strong features of your work:**

**Areas for improvement:**

**Marks Awarded:**

Contents

[A. Ethical, Legal, Social, and Professional Concerns of IoT 4](#_Toc191916083)

[B. Perspectives and Arguments from Other Writers on IoT Ethics, Legal, Social, and Professional Concerns 8](#_Toc191916084)

[C. Recommendations to Mitigate Ethical, Legal, Social, and Professional Issues in IoT 12](#_Toc191916085)

[D. The Importance of an Ethical Approach in IoT and Professional Development 17](#_Toc191916086)

### Ethical, Legal, Social, and Professional Concerns of IoT

The Internet of Things (IoT) is a transformative technology that facilitates the interconnection of a diverse array of physical objects like electronic sensors switches motors and mechanical peripherals to the internet, enabling data collection, sharing, and analysis. IoT is revolutionizing industries by enhancing operational efficiency, improving consumer experiences, and creating novel avenues for innovation. However, the rapid proliferation of IoT technologies has given rise to numerous ethical, legal, social, and professional concerns that necessitate critical examination to ensure responsible implementation. This section evaluates these concerns through the application of relevant ethical principles, legislative acts, and professional codes of conduct to ensure that IoT technologies serve the public interest and uphold individual rights.

#### 1. Ethical Concerns in IoT

Privacy is arguably the most prominent ethical concern in the IoT ecosystem. As IoT devices collect vast amounts of personal data, including sensitive information such as location, health data, and daily activities, ensuring that this data is adequately protected is essential. Ethical guidelines dictate that users must be fully informed about what data is being collected, how it will be used, and who will have access to it. The principle of informed consent is crucial in IoT contexts. Users should have a clear understanding of the data practices and should be allowed to opt-in or opt-out freely (Binns, 2018). However, many IoT devices collect data without explicit consent, leading to ethical dilemmas regarding whether users are sufficiently aware of the data collection processes, particularly when the data is being sold to third-party advertisers or used for commercial gain.

One of the core ethical issues with privacy in IoT is the fact that most users are unaware of the scale of data collection. For instance, devices such as smart thermostats, refrigerators, and fitness trackers monitor users' behaviors, preferences, and routines, often sharing this information with third-party service providers. This raises significant concerns about the extent to which users' private lives are exposed, often without their knowledge. IoT companies may assert that this data is anonymized and used solely for improving user experiences; however, there is no guarantee that this data cannot be re-identified and misused, creating potential vulnerabilities for individuals (Pinto, 2024)

Data security represents another significant ethical challenge. The interconnectedness of IoT devices means that breaches in one device can potentially affect many others within the same ecosystem. With personal data being transmitted over networks, the principle of non-maleficence requires that adequate safeguards be implemented to prevent malicious attacks. Many IoT devices lack robust encryption or rely on outdated security protocols, making them vulnerable to cyberattacks. Cybersecurity experts recommend using end-to-end encryption, multi-factor authentication, and regular security updates to secure IoT devices from potential threats (Mohammad, 2020). Failure to ensure data security not only compromises individual privacy but can also damage the reputation of companies involved in the development and deployment of IoT technologies.

Another ethical concern is related to autonomy and fairness in decision-making processes. IoT systems often rely on algorithms to make decisions based on the data they collect. If these algorithms are not designed carefully, they may inadvertently reinforce existing biases. For example, in health IoT devices, an algorithm that assumes a certain user demographic could unintentionally discriminate against individuals from different backgrounds (Sweeney, 2018). Ethical frameworks require IoT developers to design algorithms that are transparent, fair, and inclusive. This can be achieved by testing algorithms on diverse datasets and regularly auditing them for fairness.

Furthermore, IoT systems may inadvertently engender a false sense of security, particularly in sectors such as healthcare, where smart devices are integrated into patient care. Users may erroneously assume that the technology is infallible or consistently reliable, without fully comprehending the limitations of the system. Developers must address these concerns through transparency and by explicitly communicating the potential risks associated with relying on IoT systems for critical decisions, such as medical diagnoses or safety measures. Transparency and accountability are fundamental to ensuring that IoT devices are ethically aligned with users' expectations. A lack of transparency can result in a situation where users do not comprehend the scope of data collection, or the way their data is utilized to generate decisions or predictions. Accountability becomes a paramount concern when IoT systems are deployed in critical areas such as healthcare or transportation. In the event of a system failure, it is essential to determine which entity bears responsibility—the manufacturer, the user, or a third-party service provider. Clear guidelines and delineation of responsibilities must be established.

#### 2. Legal Concerns in IoT

Legal concerns in IoT predominantly pertain to data ownership, privacy rights, and liability. A primary legal issue involves determining the ownership of data collected by IoT devices. The data generated by these devices can be highly valuable, leading to legal disputes regarding ownership and usage rights. In numerous instances, IoT manufacturers assert ownership over the data, while consumers may contend that the data they generate belongs to them. This ambiguity necessitates clear data protection laws that delineate the rights of consumers over their personal data. The General Data Protection Regulation (GDPR) represents a significant effort to regulate data privacy, but its application outside of the European Union remains inconsistent (Lu, 2023) (Gurumurthy, 2020) Different regions have varying legal standards, leading to potential jurisdictional issues in global IoT systems. Consequently, there is an increasing need for universal standards and frameworks to regulate data usage and ownership in the IoT industry.

A significant legal challenge pertains to data retention and data minimization principles. In many instances, IoT devices continuously collect and store data even after it is no longer required for the specific purpose for which it was collected. This raises concerns regarding the appropriate duration for retaining personal data and the necessity of retaining certain data points. For example, in the context of smart homes, retaining data on users' movements for years after they vacate the premises may not be justified, raising questions about potential violations of data protection laws. Consequently, legal experts argue that IoT devices must incorporate data lifecycle management policies that comply with laws such as GDPR, ensuring data is not stored longer than necessary (Lidia Fotia, 2023)

Liability constitutes another critical legal concern, particularly in cases where IoT devices malfunction or cause harm. If a smart home device malfunctions and causes damage to property, it raises the question of legal responsibility—whether it lies with the manufacturer, the service provider, or the consumer. The complex network of devices, service providers, and third parties involved in IoT systems complicates the attribution of liability. Furthermore, IoT devices often operate autonomously, meaning they could cause harm even without human intervention. The legal concept of strict liability may need to be extended to IoT systems to address these issues, ensuring that manufacturers are held accountable for any harm caused by their products (Lidia Fotia, 2023)

Intellectual Property (IP) rights also play a crucial role in the legal landscape of IoT. As IoT devices often rely on proprietary software, firmware, and hardware, legal disputes over IP ownership are common. These disputes can involve patent infringements or challenges to the terms of licenses for software components. As IoT devices integrate more third-party software and services, establishing clear IP rights and usage terms becomes critical. The IoT industry also requires clearer guidelines on open source versus proprietary software to promote innovation while protecting the intellectual property rights of developers (Mohammad, 2020)

#### 3. Social Concerns in IoT

The social implications of IoT technology are extensive and multifaceted. One of the most significant societal concerns is the digital divide. While IoT technologies have the potential to enhance quality of life by increasing service efficiency and personalization, they are not equally accessible to all segments of society. Low-income populations or residents of rural areas may lack access to the requisite infrastructure for IoT devices, such as stable internet connections or electricity. This disparity could further exacerbate inequality, placing vulnerable populations at a disadvantage in terms of access to healthcare, education, or economic opportunities that IoT could offer (Binns, 2018)

Furthermore, IoT devices are increasingly being utilized for surveillance, raising concerns regarding privacy and individual liberty. While IoT systems offer benefits such as improved security and public safety, they also enable continuous tracking and monitoring of individuals. For instance, smart cameras in residential or public spaces could be employed to collect real-time data on individuals' movements, potentially infringing upon personal freedoms. Governments and corporations are increasingly interested in utilizing IoT systems for mass surveillance, which can lead to a surveillance society where individuals have limited control over the data collected about them. In this context, ethical concerns regarding consent, control, and transparency become increasingly critical. Legislation and regulations must be implemented to prevent unnecessary surveillance and ensure that data collection is strictly for justified purposes (Gurumurthy, 2020).

Another significant societal issue is the impact of IoT on employment. Automation powered by IoT technology can displace workers in various industries, such as manufacturing, logistics, and retail. While IoT can lead to increased efficiency and reduced operational costs, it can also result in job losses as human labor is replaced by automated systems. IoT companies and governments must balance technological advancement with job creation and retraining programs to facilitate workers' transition to new roles in the evolving economy (Zhou, 2020).

#### 4. Professional Concerns in IoT

From a professional perspective, IoT developers must adhere to ethical codes of conduct and ensure that their technologies are designed, developed, and deployed in ways that prioritize the public good. The Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM) provide comprehensive codes of ethics for professionals in the field. These codes emphasize principles such as transparency, honesty, integrity, and accountability in the design and development of IoT systems. Engineers and developers must also consider the long-term implications of their work, ensuring that IoT technologies do not cause harm or create undue risks for users (IEEE, 2025).

Another professional concern is the necessity for ongoing education and awareness in IoT. As the field of IoT continues to evolve, it is crucial for professionals to remain current with the latest trends, security challenges, and regulatory developments. Continuous professional development through training and certification programs ensures that IoT developers are prepared to address emerging ethical, legal, and social challenges (Zhou, 2020). Professionals should also participate actively in discussions regarding the social and ethical implications of IoT technology, as the responsible design and use of IoT will depend on their commitment to upholding ethical principles.

Lastly, IoT professionals must foster user trust in IoT technologies. As IoT devices become increasingly integrated into critical areas such as healthcare, autonomous transportation, and personal security, user confidence in these systems is paramount. Trustworthy design, which involves creating secure, transparent, and user-friendly systems, is essential to building this confidence (Zeng, 2018)Professional codes of conduct emphasize the necessity of creating products that are not only functional but also safe, equitable, and aligned with societal values.

### Perspectives and Arguments from Other Writers on IoT Ethics, Legal, Social, and Professional Concerns

The ethical, legal, social, and professional concerns surrounding the Internet of Things (IoT) have been widely debated by researchers and industry experts. Various perspectives provide insights into the challenges and potential solutions for addressing issues related to privacy, liability, bias, and social impact. This section evaluates arguments made by other scholars and professionals on these concerns.

1. **Privacy and Data Protection Concerns**

Privacy remains one of the most critical ethical and legal concerns in IoT. (Zeng, 2018)asserts that IoT manufacturers must incorporate privacy-by-design principles into their products. This means that privacy measures should not be an afterthought but an integral part of the product’s architecture. Zeng also advocates for user-controlled privacy settings, where consumers can choose the level of data, they are comfortable sharing.

Similarly, (Binns, 2018)emphasizes that data protection laws such as the General Data Protection Regulation (GDPR) play a vital role in protecting consumers from privacy breaches. He argues that IoT developers must ensure compliance with data minimization principles, which require collecting only the data necessary for device functionality. Failure to comply with such regulations has led to lawsuits and penalties for several companies.

(Mann, 2018) highlights the growing risk of mass surveillance due to IoT devices collecting real-time location and behavioral data. Smart home devices, security cameras, and even wearable technology continuously monitor users, often sharing data with third-party service providers. Mann warns that such practices can lead to potential abuses by governments and corporations, ultimately infringing on individuals’ right to privacy.

On the other hand, (Solove, 2020) argues that privacy concerns should not hinder technological progress. While acknowledging the risks, he suggests that consumers must also take responsibility for their data by adjusting device settings and using privacy-enhancing technologies like Virtual Private Networks (VPNs) and encrypted communication.

1. **Liability and Accountability in IoT**

Determining liability for IoT failures is a complex legal challenge. (Harrison, 2017) argue that the legal landscape needs to adapt to the complexities of IoT technologies. Current liability laws were not designed with autonomous systems in mind, and as IoT devices become more sophisticated, determining liability will become increasingly difficult. They suggest that a new legal framework must be established, one that accounts for the unique nature of IoT systems.

For example, in the case of autonomous vehicles, if an IoT-enabled self-driving car causes an accident, determining whether the fault lies with the manufacturer, software developer, or user becomes challenging. While traditional legal principles hold manufacturers responsible for defective products, IoT systems often involve multiple stakeholders, including third-party software providers and cloud service companies (Goff, 2019)

(Dixon, 2019) argues that smart contracts and blockchain technology could help address accountability issues by creating transparent records of actions taken by IoT devices. This would help resolve disputes by providing verifiable logs of decisions made by the device. However, he also acknowledges that integrating such solutions into mainstream IoT development requires significant technical and legal reforms.

Furthermore, (Lipton, 2021) suggests that manufacturers should adopt strict liability policies, ensuring that any harm caused by IoT devices is automatically attributed to the manufacturer unless proven otherwise. This approach would encourage companies to prioritize safety and security measures during development.

1. **Bias and Discrimination in IoT Systems**

Another pressing ethical concern in IoT is algorithmic bias, particularly in artificial intelligence (AI)-driven IoT devices. (Sweeney, 2018) discusses the risks of bias in IoT systems, noting that many IoT applications, particularly those used in healthcare and hiring, rely on algorithms that may perpetuate existing societal biases.

For instance, if a smart hiring system analyzes job applicants' past experiences and demographics, it may inadvertently favor certain groups over others. This can lead to discrimination and exclusion of underrepresented communities. Sweeney calls for more inclusive data collection practices to ensure that IoT systems are equitable and free from discrimination.

Similarly, (Noble, 2019) examines the racial and gender biases embedded in IoT-based facial recognition technology. She found that many facial recognition systems exhibit lower accuracy when identifying individuals from minority groups, leading to concerns about wrongful identification and discriminatory surveillance practices. She argues that regulatory oversight is necessary to ensure fairness in algorithmic decision-making.

(Zhou, 2020) suggest that one way to mitigate bias in IoT systems is to use explainable AI (XAI), which provides transparency into how IoT algorithms make decisions. This approach would allow researchers and developers to audit AI behavior and identify potential biases before deployment.

1. **Social Impact of IoT**

The widespread adoption of IoT has far-reaching social implications. (Gurumurthy, 2020) highlights the issue of the digital divide, emphasizing that IoT should be designed with inclusivity in mind. She stresses that governments and organizations must invest in infrastructure to ensure that IoT technologies reach all populations, particularly in rural or underdeveloped regions.

(Center, 2021) reports that while IoT adoption is increasing globally, access to high-speed internet remains a major barrier in low-income communities. Without adequate infrastructure, the benefits of IoT may be unequally distributed, leading to technological inequality where only wealthy individuals or developed nations can leverage its advantages.

In contrast, (Greenfield, 2021) argues that IoT could help bridge the digital divide by enabling low-cost smart solutions for developing regions. He cites examples of smart agriculture in Africa, where IoT sensors assist farmers in optimizing irrigation and crop yields. While challenges exist, Greenfield believes that public-private partnerships can play a crucial role in ensuring IoT benefits all communities.

Another social concern is the impact of IoT on employment. Automation powered by IoT technology has the potential to displace workers in various industries, including manufacturing, logistics, and retail (Brynjolfsson, 2018) While IoT can increase efficiency and reduce operational costs, it also raises concerns about job losses and worker displacement.

(Ford, 2019) argues that governments should invest in reskilling programs to help workers transition to new technology-driven roles. He emphasizes that rather than viewing automation as a threat, societies should see it as an opportunity to upskill workers and create new economic opportunities.

1. **Professional Ethics in IoT Development**

IoT developers and engineers must adhere to professional codes of ethics to ensure responsible development. The IEEE Code of Ethics outlines principles such as honesty, integrity, transparency, and accountability in technology development. Professionals working with IoT must prioritize user safety, privacy, and security when designing products. (IEEE, 2025)

(Weber, 2020) emphasizes that continuous education and professional development are essential in the IoT field. He notes that since IoT technology is evolving rapidly, developers must stay updated with the latest ethical standards, security threats, and legal frameworks to build responsible and ethical systems.

Furthermore, (Floridi, 2021) argues that ethical AI governance should be a key focus for IoT professionals. He calls for interdisciplinary collaboration between technologists, policymakers, and ethicists to ensure IoT systems align with human rights and societal values.

**Conclusion**

The ethical, legal, social, and professional concerns surrounding IoT have been extensively discussed by scholars. Privacy and data protection remain major concerns, with researchers advocating for privacy-by-design and stronger regulations like GDPR. Legal challenges, particularly in liability and accountability, require new legal frameworks to address the complexities of IoT systems. Algorithmic bias in IoT can lead to discrimination, highlighting the need for fair and transparent AI models. Social challenges, including the digital divide and job displacement, require government and industry collaboration to ensure IoT benefits all communities. Lastly, IoT professionals must follow ethical codes of conduct and continue their education to ensure responsible development. Addressing these challenges will be key to maximizing the benefits of IoT while minimizing its risks.

### Recommendations to Mitigate Ethical, Legal, Social, and Professional Issues in IoT

The Internet of Things (IoT) has brought significant benefits but also raised ethical, legal, social, and professional concerns. To address these issues effectively, the following detailed recommendations should be considered:

1. **Enhancing Data Security and Privacy**

One of the most critical concerns in IoT is the security and privacy of user data. IoT devices constantly collect, process, and transmit sensitive information, making them vulnerable to cyberattacks, unauthorized access, and data breaches. To mitigate these risks, the following measures should be implemented:

a. Implement Strong Encryption Techniques

Encryption ensures that data transmitted between IoT devices and servers remains secure. Developers should use advanced encryption protocols such as:

* AES (Advanced Encryption Standard) – a widely used encryption method for securing IoT communications.
* TLS/SSL (Transport Layer Security / Secure Sockets Layer) – ensures secure communication between IoT devices and cloud platforms.

b. Use Privacy-Enhancing Technologies (PETs)

To minimize privacy risks, IoT developers should integrate technologies that protect user identities and limit data exposure:

* Differential Privacy – adds statistical noise to data to prevent individual identification (Dwork, 2008).
* Anonymization Techniques – remove personally identifiable information before storing or sharing data.

c. Give Users More Control Over Their Data

Users should have control over how their data is collected, stored, and shared. Companies should:

* Provide clear options for users to opt out of data collection.
* Allow users to delete their data permanently upon request.
* Implement privacy dashboards where users can manage their data preferences.

d. Regular Security Audits

IoT manufacturers should conduct regular security audits and penetration testing to identify and fix vulnerabilities before they are exploited by hackers (Floridi, 2021)

1. **Establishing Clear Legal Guidelines**

Governments play a crucial role in regulating IoT devices to ensure they are safe, secure, and ethically designed. Without proper regulations, companies may exploit user data, leading to privacy violations and security breaches. To prevent this, the following actions should be taken:

a. Create Comprehensive IoT Regulations

Many countries have adopted data protection laws, but there is a need for specific IoT-focused regulations. Governments should introduce laws that:

* Require strong cybersecurity measures for IoT devices.
* Establish liability frameworks in case of security breaches.
* Mandate data protection measures similar to the General Data Protection Regulation (GDPR) in the European Union.

b. Standardized Compliance Requirements

Companies should be required to follow global standards for IoT security and privacy, such as:

* ISO/IEC 27001 – for information security management.
* NIST Cybersecurity Framework – for securing IoT ecosystems.

c. Enforce Accountability and Penalties

Companies that fail to comply with security and privacy laws should face strict fines and penalties. For instance, GDPR fines can reach up to €20 million or 4% of a company’s global annual revenue (Commission, 2021).

1. **Promoting Transparency**

Many IoT users do not fully understand how their data is collected, stored, or used. To ensure ethical use of IoT technologies, companies should enhance transparency through the following steps:

a. Clear and Understandable Privacy Policies

Privacy policies should be:

* Written in simple language instead of complex legal terms.
* Easily accessible on company websites and device interfaces.
* Regularly updated to reflect changes in data usage practices.

b. Explain Data Usage to Users

IoT companies should provide clear explanations of:

* What data is collected? (e.g., location, voice recordings, biometric data)
* Why is it collected? (e.g., improving services, targeted advertising)
* Who has access to it? (e.g., third-party companies, advertisers)

c. Implement User-Friendly Data Management Tools

* Consent Management Platforms (CMPs) – allow users to review and change their privacy settings.
* Automated Data Deletion Options – enable users to set automatic deletion for stored data.

1. **Addressing Bias in IoT Algorithms**

Many IoT applications rely on artificial intelligence (AI) and machine learning (ML) algorithms, which can inherit biases from the data used to train them. Bias in IoT algorithms can lead to discrimination, unfair treatment, and inaccurate decision-making. To address this, the following measures should be taken:

a. Regular Bias Audits and Testing

Developers should conduct regular bias audits to check for:

* Racial, gender, or socio-economic biases in data collection and processing.
* Unintended discrimination in AI-based decision-making.

b. Use Diverse and Representative Datasets

AI models should be trained on datasets that represent different:

* Demographic groups.
* Geographic regions.
* Economic backgrounds.

c. Diverse Development Teams

Having diverse teams in IoT development can help:

* Identify potential blind spots in algorithms.
* Ensure fairness and inclusivity in AI-powered IoT systems.

d. Ethical AI Guidelines

Companies should follow ethical AI frameworks, such as:

* IEEE Ethically Aligned Design (IEEE, 2025).
* AI Fairness 360 – an open-source toolkit for bias detection.

1. **Fostering Inclusivity in IoT Adoption**

IoT technology should be accessible to all users, including those in underserved communities. The digital divide remains a major challenge, preventing equal access to IoT benefits. To bridge this gap, the following steps should be taken:

a. Government Subsidies for IoT Devices

Governments should provide financial support to:

* Low-income households to afford IoT devices.
* Schools and educational institutions to integrate IoT learning programs.

b. Digital Literacy Programs

Many people lack the knowledge to use IoT devices effectively. Digital literacy programs should be:

* Offered in schools and universities.
* Provided as community workshops.
* Available online for free.

c. Design IoT Devices for Accessibility

IoT products should be designed to accommodate users with:

* Visual impairments (voice-assisted navigation).
* Hearing impairments (text-based interfaces).
* Physical disabilities (adaptive controls).

d. Expand IoT Infrastructure to Rural Areas

Many rural areas lack the network infrastructure needed for IoT connectivity. Governments should:

* Invest in 5G and broadband expansion projects.
* Partner with private companies to build IoT-ready networks.

**Conclusion**

The rapid growth of IoT technology presents significant challenges in terms of security, privacy, regulation, transparency, fairness, and accessibility. By implementing strong encryption methods, legal frameworks, transparency measures, bias audits, and inclusive policies, the ethical, legal, social, and professional concerns surrounding IoT can be mitigated. Collaboration between governments, businesses, and users is essential to ensure that IoT remains safe, fair, and beneficial for society.

### The Importance of an Ethical Approach in IoT and Professional Development

**Introduction**

The rapid expansion of the Internet of Things (IoT) has transformed the way people interact with technology, enabling smart cities, connected healthcare, and industrial automation. However, as IoT adoption increases, ethical concerns surrounding privacy, security, transparency, and fairness become more critical. A strong ethical approach is essential to ensure that IoT technologies benefit society while mitigating risks such as data misuse, algorithmic bias, and surveillance concerns (Floridi, 2021) For IT professionals, ethical decision-making is not only a moral responsibility but also a crucial factor in career growth, legal compliance, and public trust.

**1. Ethical Responsibilities in IoT Development**

IoT professionals have a duty to design and implement technologies that uphold ethical principles. Key responsibilities include:

a. Protecting Privacy and User Data

IoT devices collect vast amounts of personal data, including location, health records, and financial information. Without strong ethical guidelines, this data can be misused for unauthorized surveillance, targeted advertising, or identity theft. Ethical developers must:

* Ensure informed user consent before collecting data (Dwork, 2008)
* Use encryption and anonymization to protect sensitive information.
* Allow users to control their data, including deletion options.

b. Ensuring Security and Preventing Harm

Cyberattacks on IoT devices can have severe consequences, including financial loss and physical harm (e.g., hacking into connected cars or medical devices). Ethical professionals should:

* Follow secure coding practices to prevent vulnerabilities.
* Regularly conduct penetration testing and security audits.
* Implement firmware updates to address emerging threats.

c. Promoting Transparency and Fairness

Users must understand how IoT systems work and how their data is used. Ethical professionals should:

* Provide clear privacy policies without complex legal jargon.
* Ensure that AI-driven IoT systems avoid discrimination based on race, gender, or socio-economic status.
* Disclose potential biases in algorithms and allow for human oversight.

**2. Professional Development and Ethical Decision-Making**

A strong ethical foundation enhances an IoT professional’s career in several ways:

a. Building Public Trust and Credibility

Consumers and businesses are more likely to adopt IoT products from companies that prioritize ethical standards. Trust is a key factor in brand reputation and user adoption. A 2021 study by the European Commission found that 72% of consumers would stop using IoT services if they felt their data was mishandled (Commission, 2021)

b. Avoiding Legal and Regulatory Risks

Non-compliance with ethical and legal standards can lead to lawsuits, fines, and reputational damage. Regulations such as GDPR and the California Consumer Privacy Act (CCPA) impose strict requirements on data collection and security. Ethical professionals proactively:

* Stay updated on global data protection laws.
* Ensure IoT compliance with legal frameworks.
* Advocate for corporate policies that prioritize ethical design.

c. Enhancing Long-Term Career Growth

Ethical professionals are valued for their integrity, decision-making, and risk management skills. Organizations prefer hiring IoT experts who:

* Follow industry codes of conduct, such as IEEE’s Ethically Aligned Design (IEEE, 2021).
* Demonstrate leadership in responsible innovation.
* Contribute to ethical discussions in IoT forums and publications.

**3. Ethical Codes and Professional Accountability**

Several organizations provide ethical guidelines for IoT professionals:

* IEEE Code of Ethics – Promotes honesty, fairness, and public welfare in technology development (IEEE, 2021)
* ACM Code of Ethics – Encourages professionals to prioritize human well-being and avoid harm ((ACM), 2022)
* ISO/IEC 27001 – Provides global standards for information security management in IoT systems.

Adhering to these ethical frameworks strengthens the credibility of IoT professionals and their contributions to society.

**Conclusion**

An ethical approach in IoT is essential for protecting privacy, security, and fairness while fostering professional integrity and career growth. By prioritizing transparency, compliance, and responsible decision-making, IT professionals not only enhance public trust but also safeguard their organizations from legal risks. As IoT continues to evolve, ethical leadership will be a defining factor in shaping the future of technology and its impact on society.

# References

(ACM), A. f. C. M., 2022. *ACM Code of Ethics and Professional Conduct.* [Online]   
Available at: https://www.acm.org/code-of-ethics  
[Accessed 31 January 2025].

Binns, R., 2018. Internet of Things: Privacy Issues, Security Challenges, and Future Solutions. *International Journal of Information Security,* 3(17), pp. 118-131.

Brynjolfsson, E. a. M., 2018. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies,* New York: W. W. Norton & Company.

Center, P. R., 2021. *Internet of Things Adoption and Global Digital Divide.* [Online]   
Available at: https://www.pewresearch.org   
[Accessed 31 January 2025].

Commission, E., 2021. *Consumer trust in IoT and data privacy.* [Online]   
Available at: https://ec.europa.eu/  
[Accessed 31 January 2025].

Commission, E., 2021. *General Data Protection Regulation (GDPR).* [Online]   
Available at: https://ec.europa.eu/  
[Accessed 31 January 2025].

Dixon, P., 2019. Smart contracts and IoT: The future of accountability?. *Technology and Society Journal,* 45(1), pp. 72-89.

Dwork, C., 2008. *Differential privacy: A survey of results,* s.l.: Theory of Cryptography Conference.

Floridi, L., 2021. Ethical AI governance in IoT: A multidisciplinary perspective. *AI & Society,* 36(3), pp. 531-546.

Ford, M., 2019. *The Rise of the Robots: Technology and the Threat of a Jobless Future,* New York: Basic Books.

Goff, B., 2019. Autonomous Vehicles and Liability: Who Pays the Price?. *Journal of Cyber Law,* 25(1), pp. 15-21.

Greenfield, A., 2021. *Radical Technologies: The Design of Everyday Life,* London: Verso.

Gurumurthy, A., 2020. The Role of IoT in the Digital Divide. *Journal of Digital Ethics,* 15(2), pp. 28-40.

Harrison, J. a. R. P., 2017. Legal Challenges in IoT: The Need for a New Liability Framework. *International Review of Law, Computers & Technology,* 31(4), pp. 289-306.

IEEE, 2021. *IEEE Code of Ethics.* [Online]   
Available at: https://www.ieee.org/about/corporate/governance/p7-8.html  
[Accessed 31 JAnuary 2025].

IEEE, 2025. *Institute of Electrical and Electronics Engineers.* [Online]   
Available at: https://www.ieee.org/about/corporate/governance/p7-8.html  
[Accessed 31 January 2025].

Lidia Fotia, F. M. D. R. G. M. S., 2023. *Security, Trust and Privacy Models, and Architectures in IoT Environments.* 1 ed. s.l.:Springer Cham.

Lipton, A., 2021. Strict Liability in IoT: A New Approach to Accountability. *Harvard Law Review,* 134(3), pp. 567-589.

Lu, Y., 2023. Security and Privacy of Internet of Things: A Review of Challenges and Solutions. *Journal of Cyber Security and Mobility,* 10(13052), pp. 2245-1439.

Mann, C., 2018. Surveillance and Smart Technologies: The IoT Privacy Dilemma. *Privacy & Security Journal,* 29(1), pp. 22-40.

Mohammad, S. M., 2020. Security and Privacy Concerns of the Internet of Things? (IoT) in IT and its Help in the Various Sectors across the World. *International Journal of Computer Trends and Technology,* 68(4), pp. 266-272.

Noble, S., 2019. *Algorithms of Oppression: How Search Engines Reinforce Racism,* New York: NYU Press.

Pinto, G. P. D. P. K. D. S. &. P. C., 2024. *A Systematic Review on Privacy-Aware IoT Personal Data Stores,* Switzerland: Basel, .

Solove, D., 2020. *Understanding Privacy. Cambridge, MA,* Cambridge: Harvard University Press.

Sweeney, L., 2018. Discrimination in AI-driven IoT: The Need for Fair Data Practices. *Journal of Technology Ethics,* 27(3), pp. 85-102.

Weber, R., 2020. Professional Ethics in IoT Development: The Role of Engineers and Designers. *Technology and Ethics Review,* 18(2), pp. 305-325.

Zeng, Z., 2018. IoT: The Good, the Bad, and the Ugly. *International Journal of Technology Ethics,* 13(2), pp. 145-158.

Zhou, Z., 2020. IoT and Data Security: A New Paradigm. *Information Security Journal,* 29(2), pp. 107-120.