INSTITUTE FOR CLIMATE LAW & SUSTAINABLE POLICY

INSTITUTE FOR CLIMATE LAW & SUSTAINABLE POLICY

THE JOURNAL OF CLIMATE LAW AND SUSTAINABLE POLICY

VOLUME 01 NO 02 ISSUE DECEMBER 2025

https://journal.iclsp.com/

Aligning Environmental Sustainability with Personal Data Protection in the Internet of Things

Janna Shafira W Apcar*, Ranim[2],

[1] *Faculty of Law, Trisakti University, Indonesia*

[2] *Faculty of Law, Trisakti University, Indonesia*

**Corresponding Author: Ranim0701@gmail.com*

ARTICLE INFO

Keywords:

Data Governance

Environmental;

Internet of Things (IoT);

Personal Data Protection

How to cite:

-

Article History:

Received: 20 February 2025

Revised: 10 November 2025

Accepted: 30 December 2025

ABSTRACT

The rapid development of the Internet of Things (IoT) has led to its widespread adoption in homes, offices, and public spaces. While IoT technologies offer efficiency, convenience, and environmental benefits, their massive deployment also raises significant concerns regarding data protection and environmental sustainability. This paper argues that responsible IoT governance requires balanced attention to both personal data security and environmental impact. From a data protection perspective, IoT systems must ensure the protection of data subjects' rights, implement secure data storage and transmission mechanisms, and establish clear legal bases for data processing. Transparency, accountability, and privacy-by-design principles are essential to maintain trust in IoT ecosystems. From an environmental perspective, IoT development must address energy efficiency, responsible resource consumption, device lifecycle management, and proper waste management, including the reduction of electronic waste (e-waste) and the promotion of recycling and circular economy practices. Without sustainable design, the environmental costs of IoT may outweigh its intended benefits. This study emphasizes the importance of aligning Environmental Sustainability Impact Assessments (ESIA) with Data Protection Impact Assessments (DPIA). Conducting both assessments simultaneously enables organizations to identify privacy, security, and environmental risks at an early stage, ensuring that IoT systems are not only legally compliant and secure, but also environmentally responsible. Integrated governance frameworks therefore play a critical role in building trustworthy, sustainable, and resilient IoT ecosystems for the future.

1. Introduction

Internet of Things ("**IoT**"), which was first introduced by Kevin Ashton in 1999, describes a future where connected devices could improve communication and enable richer interaction between people and the digital world. Today, IoT is most commonly implemented in industrial and commercial sectors, linking a wide spectrum of "smart" objects, from everyday wearables and household devices to complex, large-scale machinery, into interconnected systems.[1]

Within this context, environmental regulation and the deployment of IoT play an increasingly important role in promoting green growth and supporting climate change mitigation. Through real-time data collection, continuous monitoring, and automated control, IoT technologies enable more efficient resource management and improved operational performance. These capabilities contribute to environmentally sustainable development while also delivering economic benefits in the form of cost reductions and productivity gains.[2]

Accordingly, IoT applications are now widely used across various industries to improve efficiency, reduce operational costs, and enhance productivity. As the technology continues to develop, further industrial IoT applications are expected to emerge. Nevertheless, despite these advantages, the implementation of IoT in industrial environments also presents significant challenges that require careful consideration.[3]

One of the challenges is that the same data-driven capabilities that make IoT valuable for environmental objectives also rely on extensive data processing. People often say personal data is the new oil, fueling the internet and powering the digital economy. However, if data is truly comparable to oil, it cannot be treated casually. It needs careful handling at every stage, collected under clear rules, used in a controlled way, stored securely, and deleted responsibly.

Just as oil has spillovers and environmental consequences, data use can create real risks and harms, so those impacts should be anticipated, mitigated, and weighed against stakeholder interests.[4]

Also, the rapid expansion of intelligent and connected devices has accelerated the adoption of the Internet of Things (IoT), making it increasingly important to understand the protection and security challenges that accompany this growth. Although IoT is often promoted as a technology that supports environmental sustainability, through improved energy efficiency, resource optimization, and environmental monitoring, its deployment may also introduce adverse impacts, including increased energy consumption and electronic waste.

Accordingly, this research seeks to examine these tensions and to identify approaches for governing IoT in a manner that aligns environmental objectives with robust personal data protection principles.

2. Research Method

This research employs a normative legal research method with a descriptive and analytical approach. The study focuses on examining legal principles, regulatory frameworks, and governance mechanisms related to the deployment of IoT technologies, particularly in the context

---

[1] Muhammad Aqeel, Fahad Ali, Muhammad Waseem Iqbal, Toqir A. Rana, Muhammad Arif, and Md. Rabiul Auwul, 'A Review of Security and Privacy Concerns in the Internet of Things', *Hindawi Security and Communication Networks*, 2022 (2022), 2 <https://doi.org/10.1155/2022/5724168>

[2] Zhang Dong and Sana Ullah, 'Towards a Green Economy in China? Examining the Impact of the Internet of Things and Environmental Regulation on Green Growth', *Sustainability*, 15.16 (2023), 12528 https://doi.org/10.3390/su151612528

[3] Hamed Taherdoost, 'Security and Internet of Things: Benefits, Challenges, and Future Perspectives', *Electronics* (MDPI), 3 <https://www.mdpi.com/journal/electronics>

[4] Bart van der Sloot, Chris Jay Hoofnagle and F. J. Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means', *Information & Communications Technology Law*, 28.1 (2019), 66 <https://doi.org/10.1080/13600834.2019.1573501>

of environmental sustainability and personal data protection. This research is conceptual in nature and does not involve empirical data collection.

The data used in this research consist of secondary sources, including international and regional regulations, policy documents, academic journals, and scholarly literature on environmental law, data protection law, and IoT governance. Key legal instruments, such as data protection regulations and environmental governance frameworks, are analyzed to identify their relevance and applicability to IoT ecosystems.

The analysis is conducted through qualitative legal analysis, involving interpretation of legal texts, identification of regulatory gaps, and assessment of how existing legal norms address the environmental and privacy challenges posed by IoT systems. A comparative perspective is also applied where relevant to highlight differences and similarities in regulatory approaches, to develop an integrated understanding of IoT governance that aligns environmental objectives with robust personal data protection principles.

3. Result and Discussion

3.1. Environmental Impact of IoT Systems

IoT systems are increasingly deployed across various sectors, including energy management, transportation, industry, and environmental monitoring. These systems rely on interconnected sensors, data transmission networks, and data analytics infrastructure, which together shape their environmental footprint. From an environmental and energy law perspective, the impact of the IoT system is inherently mixed, as sustainability benefits coexist with new environmental risks.

One of the primary environmental advantages of IoT systems lies in their ability to improve energy efficiency. Smart meters, automated control systems, and sensor-based monitoring enable more efficient use of electricity by optimizing energy consumption patterns in buildings and industrial processes. Studies indicate that IoT-enabled energy management systems can reduce overall energy demand and facilitate the integration of renewable energy sources, contributing to lower greenhouse gas emissions.[5]

IoT systems also play a significant role in environmental monitoring and resource management. Sensors used for air quality measurement, water management, and waste monitoring provide continuous and accurate environmental data, allowing for early detection of pollution and inefficiencies. Such data driven monitoring supports regulatory compliance and enhances environmental governance by improving transparency and accountability.[6]

Despite these benefits, IoT systems generate environmental externalities that are often overlooked. The manufacturing and deployment of IoT devices require raw materials and energy-intensive processes, resulting in embodied carbon emissions. Life-cycle assessment studies show that the environmental cost of producing sensors and edge devices may offset part of the energy savings achieved during their operational phase.[7]

Furthermore, the environmental impact of IoT systems extends beyond individual devices to the digital infrastructure that supports them. Data transmission, cloud computing, and large-scale data storage significantly increase energy consumption, particularly in data centers operating continuously. These indirect energy impacts are rarely considered in traditional environmental impact assessments, creating regulatory blind spots within existing environmental law frameworks.

[5] S. Misra et al., Green IoT: Energy Efficiency and Sustainable Smart Cities, IEEE Communications Magazine, Vol. 53, No. 1 (2015).

[6] M. Rathore et al., Urban Planning and Smart City Decision Management Empowered by IoT, Sustainable Cities and Society, Vol. 32 (2017).

[7] J. Pirson & D. Bol, Assessing the Embodied Carbon Footprint of IoT Edge Devices Using Life-Cycle Assessment, Journal of Cleaner Production, Vol. 394 (2023).

Liu and De Giovanni (2019) analyze the economic, environmental, and social impacts of investments in Industry 4.0 technologies, particularly robotics and the IoT. Their findings show that digital technologies can improve production efficiency and help firms reduce emissions at the process level by lowering waste, scrap rates, and energy use per unit of output.

However, they identify an "eco-innovation paradox," while efficiency improvements reduce emissions per product, digitalization also increases market access and demand, leading to higher production volumes. As a result, total emissions may rise, offsetting environmental gains and causing stagnation in overall environmental performance.

This mixed outcome is further reinforced by the energy-intensive nature of digital infrastructure. Many IoT architectures rely on cloud-based infrastructure, such as OpenIoT, which supports the Infrastructure as a Service (IaaS) model.[8] While cloud computing enables scalability and advanced data analytics, it also depends on large data centers that consume significant amounts of electricity and contribute to global carbon emissions.

Consequently, the literature emphasizes that Industry 4.0 and IoT technologies can only deliver net environmental benefits if they are accompanied by systemic changes in supply chains. These include green investments in products, production processes, logistics networks, and energy-efficient digital infrastructure, rather than relying on digitalization alone.[9]

In addition, current environmental assessment approaches tend to focus on the functional benefits of IoT systems while insufficiently addressing their cumulative and life-cycle impacts. Sustainability claims associated with IoT deployment often emphasize efficiency gains without fully accounting for long-term energy use, electronic waste, and carbon emissions. This highlights the need for a more comprehensive regulatory approach that evaluates IoT systems as part of the environmental burden they create, rather than solely as tools for environmental improvement.

A practical example of IoT implementation can be seen in smart energy management systems used in commercial buildings. Smart sensors and connected meters monitor electricity usage in real time and automatically adjust lighting, heating, and cooling systems to optimize energy efficiency. For instance, smart thermostats can reduce unnecessary energy consumption by adjusting temperatures based on occupancy patterns. While such systems contribute to reducing greenhouse gas emissions and improving environmental sustainability, they also rely on continuous data collection and cloud-based processing, which increases energy consumption in data centers and creates indirect environmental impacts that are often overlooked.

3.2. Safeguarding Personal Data in IoT Ecosystems

The existing personal data protection laws and regulations universally acknowledge the fundamental right of individuals to safeguard their personal data. Personal data protection is foundational legal and social concepts that help individuals maintain control over who can access and use information about them. In the European Union, the General Data Protection Regulation (GDPR) defines personal data as any information relating to an identified or identifiable natural person (Article 4). Put simply, if information can directly or indirectly identify someone, it may qualify as personal data and should be protected.

Comparable concepts appear in other frameworks, including the OECD privacy principles, the California Consumer Privacy Act (CCPA), and Canada's Personal Information Protection and

[8] Theodoros Anagnostopoulos, Arkady Zaslavsky, Kostas Kolomvatsos, Alexey Medvedev, Pouria Amiran, Jeremy Morley and Stathes Hadjiefthymiades, 'Challenges and Opportunities of Waste Management in IoT-Enabled Smart Cities: A Survey', *ResearchGate* (2017) <https://www.researchgate.net/publication/315977130_Challenges_and_Opportunities_of_Waste_Management_in_IoT-Enabled_Smart_Cities_A_Survey>

[9] Pier Giacomo Cardinali and Pietro De Giovanni, 'Responsible Digitalization through Digital Technologies and Green Practices', *Corporate Social Responsibility and Environmental Management*, 29 (2022), 986 <https://doi.org/10.1002/csr.2249>

Electronic Documents Act (PIPEDA). Across many regimes, personal data is closely associated with Personally Identifiable Information (PII), information that identifies or can reasonably be linked to an individual. Examples of particularly sensitive identifiers include government-issued numbers (e.g., social security or insurance numbers), driver's license numbers, and biometric data.[10]

However, these global data protection regimes were primarily designed to provide general protection safeguards and do not yet offer explicit guidance on how such principles should be implemented within highly interconnected, energy-efficient. As a result, the application of traditional data protection provisions to complex IoT-driven environments remains ambiguous, highlighting a regulatory gap that warrants further examination.

The use of IoT technologies often happens without users giving clear or explicit consent. The legal basis for collecting and processing personal data becomes unclear, and many users never see a proper privacy notice when they start using the product. This lack of transparency creates serious concerns about how securely personal data is stored in IoT systems, especially because many of the data types involved can be highly sensitive.

Biometric information, such as fingerprints, facial recognition data, and voice patterns, is considered sensitive personal data in many data protection regulations. However, IoT users often do not receive proper tools or channels to object, ask questions, or exercise their data protection rights. In many situations, individuals also do not have a real chance to give informed consent, because the collection and use of their data happens automatically within IoT devices and ecosystems.

This gap between what regulations require and what actually happens in practice shows a clear imbalance of power between IoT service providers and end-users. It also highlights the urgent need for stronger safeguards, more transparent consent processes, and solid data-governance standards that are specifically designed for IoT environments.

Beyond the issue of consent, machine-to-machine communication introduces significant challenges in personal data protection. In many IoT devices, especially those without a screen, users have no visibility into what types of personal data are being collected, how the data is processed, or where the stored data is transmitted. This limitation makes it difficult to ensure transparency. Without clear information, users lack control and understanding over the security of their personal data, increasing the risk of harmful data breaches. This situation illustrates that it still falls short in applying the principles of accountability and transparency, which should be fundamental in managing personal data within the IoT ecosystem.

Furthermore, the lack of clarity regarding what personal data is stored within IoT devices creates its own set of risks. Vulnerabilities in these devices can allow hackers or other unauthorized parties to access the data. Because IoT data is often highly personal and closely tied to various privacy concerns, lawsuits seeking to hold manufacturers accountable for such security weaknesses have been increasing.[11]

One of the most significant cases occurred in October 2016, when a large-scale Distributed Denial of Service (DDoS) attack targeted the service provider Dyn. The attack was carried out using an IoT botnet powered by malware known as *Mirai*, which infected vulnerable devices by exploiting default usernames and passwords. Once compromised, these devices, such as digital cameras and DVR players, were used to flood Dyn's servers with traffic, causing widespread outages across major platforms including Twitter, Netflix, Reddit, CNN, and *The Guardian*.

In 2017, the United States Food and Drug Administration (FDA) reported serious security flaws in certain medical devices, including pacemakers and defibrillators. These vulnerabilities

---

[10] S. Shahriar, S. Allana, S. M. Hazratifard, and R. Dara, 'A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle', *IEEE Access*, 11 (2023), 61831–61832 <https://doi.org/10.1109/ACCESS.2023.3287195>

[11] Samantha V. Ettari, 'Handling Internet of Things Data in Litigation', *E-Discovery Bulletin*, Kramer Levin Naftalis & Frankel LLP, December 2018/January 2019 <https://www.hsfkramer.com/kl-pdfs/4/6/46579.pdf>

allowed unauthorized parties to potentially interfere with the functioning of the devices, manipulate electrical shocks, alter heart pacing, or drain batteries, thereby posing direct risks to patients' health and safety.

Similarly, security researchers affiliated with IBM demonstrated the feasibility of remotely controlling an Internet-connected vehicle. In this case, a team successfully took control of a Jeep SUV through its internal communication system (CAN bus). By exploiting weaknesses in the vehicle's firmware and mobile network connectivity, the researchers were able to manipulate driving functions such as steering and acceleration, potentially endangering both passengers and the public.

These cases illustrate that IoT affects personal data and user behavior in two fundamental ways. First, IoT-enabled devices collect significantly larger volumes of data than traditional non-connected devices, including information about users' habits, movements, and activities. Second, IoT systems are inherently more exposed to security breaches and unauthorized access due to their continuous connectivity and complex infrastructures. As a result, IoT security challenges are not only more technologically demanding but also raise increasingly complex legal and regulatory concerns.[12]

Looking ahead, personal data governance is essential here to ensure the secure evolution of IoT technologies. This requires the implementation of comprehensive policies, regular Data Protection Impact Assessments (DPIAs), and clear standards for upholding data subject rights. Additionally, maintaining thorough documentation and procedures for data breach incidents is crucial. By prioritizing these measures, organizations can build trust, ensure security, and take responsibility seriously as they move forward with new IoT developments.

In Indonesia, Electronic Traffic Law Enforcement (ETLE) systems provide a clear example of how IoT technologies intersect with both environmental sustainability and personal data protection concerns. These systems use Internet-connected cameras to monitor traffic violations, reduce congestion, and improve traffic efficiency, which may contribute to lower vehicle emissions and environmental benefits. However, ETLE cameras also collect and process personal data, including vehicle identification and movement information. This demonstrates that IoT deployment simultaneously creates environmental benefits and data protection risks. Therefore, conducting both Environmental Sustainability Impact Assessments and Data Protection Impact Assessments is essential to ensure that such systems operate in a manner that is both environmentally sustainable and compliant with personal data protection principles.

3.3. Aligning Environmental Sustainability Impact Assessment with Personal Data Impact Assessment

The challenges highlight the importance of coordinated governance, shared technical standards, and continuous institutional learning. These elements are essential to ensure that IoT systems work across sectors and genuinely support long-term sustainability goals, while keeping the personal data secured.[13]

The next stage of the analysis will involve piloting the following elements as modules within the DPIAs and Environmental Sustainability Impact Assessment (ESIAs) frameworks. The collaborative model for IoT data governance is needed, as it relies on four key drivers, which are consumer awareness and education, industry accountability and responsibility, regulatory institutions, and a clear regulatory framework. To establish a more comprehensive IoT and personal

---

[12] Mahmood Al-Zoube, 'Data Protection and Privacy in the Age of Big Data: Ethical and Regulatory Challenges', *Baltic Journal of Real Estate Economics and Construction Management*, 8 (2020), 176–177 < https://doi.org/10.2478/bsrj-2020-0033>

[13] Giuseppe Lanfranchi, Antonio Crupi and Fabrizio Cesaroni, 'Internet of Things (IoT) and the Environmental Sustainability: A Literature Review and Recommendations for Future Research', *Corporate Social Responsibility and Environmental Management* 2025, 7664 <https://doi.org/10.1002/csr.2996>

data protection ecosystem, broad strategies must be implemented, though this requires the commitment of all stakeholders.

Regulations developed need to be flexible and adaptable to the rapid advancements in technology. It will include updating of existing regulations that are needed in order to address the new threats and stricter measures when dealing with data breaches.

As the GDPR has influenced the developments of personal data protection, especially Law Number 27 Year 2022 regarding Personal Data Protection, it is reasonable to expect that the key concerns on consumer data protection, through privacy-by-design and privacy-by-default, may be adopted to suit local requirements.[14]

Comprehensive Data Governance – as organizations also increasingly rely on data governance frameworks, which provide structured approaches to managing and protecting personal data. Such frameworks help ensure legal compliance, strengthen security, and promote ethical data use by defining clear policies, roles, and controls that safeguard data integrity and quality.[15]

Those frameworks can be introduced and applied on four levels, namely, the devices (hardware), channels and methods of communication, cloud and storage platform, and lifecycle management which are associated with the perspectives of risk management, policies, and auditing, awareness, and data protection impact assessment.

Vulnerability Management – organizations should also implement continuous vulnerability management programs. These programs should systematically identify, monitor, and remediate security weaknesses that emerge over time, including risks associated with outdated operating systems, firmware, or antivirus software.

As identification and monitoring technologies become more deeply embedded in everyday life, the rights to data protection must be carefully balanced against functional efficiency and technological innovation. Accordingly, effective IoT governance should integrate security-by-design and ongoing risk assessment to ensure that smart environments remain safe, trustworthy, and suitable for daily use.[16].

Customer Awareness – customers should prioritize reputable and accountable suppliers, as established manufacturers are generally more likely to comply with data protection and cybersecurity regulations. In contrast, low-cost products from unknown vendors may lack essential safeguards and could present increased security and privacy risks. Additionally, consumers are encouraged to actively adjust their device settings to enhance security and privacy.

Sustainability by Design – systems should be intentionally designed to reduce energy consumption and resource use at both the individual user level and across the entire system. This requires considering efficiency from the earliest design stage rather than treating sustainability as an afterthought.

Resilience by Design – system architectures should anticipate potential points of failure and evaluate how such failures might affect users. Particular attention should be given to whether disruptions could disproportionately impact vulnerable groups, including children, older persons, individuals with disabilities, and those with limited digital literacy.

Interoperability by Design – unlike conventional personal device ecosystems, Internet of Things (IoT) environments consist of both portable devices and technologies embedded within physical spaces. Lack of compatibility across platforms can create inconvenience, inefficiency, and

---

[14] Yasser Al-Hamadi, Fatimah Al Ghamdi, Mohammed Gutub and Ahmad M. Youssef, 'Smart Cities Adoption: A Framework for Sustainable Development', *Sustainability*, 14.16 (2022), 17 <https://doi.org/10.3390/su14169893>

[15] Sivananda Reddy Julakanti, Naga Satya Kiranmayee Sattiraju and Rajeswari Julakanti, 'Data Protection through Governance Frameworks', *Journal of Computational Analysis and Applications*, 31.1 (2023), 158

[16] Mahmood Al-Zoube, 'Data Protection and Privacy in the Age of Big Data: Ethical and Regulatory Challenges', *Baltic Journal of Real Estate Economics and Construction Management*, 8 (2020), 177–178 <https://doi.org/10.2478/bsrj-2020-0033>

technological lock-in, for example, when devices designed for one ecosystem cannot function within another. Regulatory principles such as data portability, reflected in frameworks like the GDPR and UU PDP, aim to promote competition and prevent market foreclosure; similar principles are therefore relevant and beneficial for IoT system design.[17]

4. Conclusion

In conclusion, the long-term viability of IoT ecosystems requires systematic data protection impact assessments to ensure that technological development aligns with principles of privacy, accountability, and lawful data processing. Such assessments enable organizations and regulators to identify risks early, implement appropriate safeguards, and maintain public trust. By embedding these evaluations within governance frameworks, policymakers can ensure that innovation proceeds in a manner consistent with fundamental rights and responsible data stewardship.

Similarly, environmental sustainability impact assessments are essential to evaluate how IoT systems affect energy consumption, resource efficiency, and ecological outcomes across their lifecycle. These assessments support evidence-based decision-making, allowing stakeholders to balance technological advancement with environmental responsibility. When integrated with regulatory standards and technical guidance, they help ensure that IoT ecosystems contribute positively to sustainability objectives while minimizing unintended environmental harm.

References

Al-Hamadi, Yasser, Fatimah Al Ghamdi, Mohammed Gutub, and Ahmad M. Youssef, 'Smart Cities Adoption: A Framework for Sustainable Development', *Sustainability*, Vol. 14, No. 16, 2022, https://doi.org/10.3390/su14169893.

Al-Zoube, Mahmood, 'Data Protection and Privacy in the Age of Big Data: Ethical and Regulatory Challenges', *Baltic Journal of Real Estate Economics and Construction Management*, Vol. 8, 2020, pp. 176–178, https://doi.org/10.2478/bsrj-2020-0033.

Anagnostopoulos, Theodoros, Arkady Zaslavsky, Kostas Kolomvatsos, Alexey Medvedev, Pouria Amiran, Jeremy Morley, and Stathes Hadjiefthymiades, 'Challenges and Opportunities of Waste Management in IoT-Enabled Smart Cities: A Survey', 2017.

Aqeel, Muhammad, Fahad Ali, Muhammad Waseem Iqbal, Toqir A. Rana, Muhammad Arif, and Md. Rabiul Auwul, 'A Review of Security and Privacy Concerns in the Internet of Things', *Security and Communication Networks*, 2022, https://doi.org/10.1155/2022/5724168.

Cardinali, Pier Giacomo, and Pietro De Giovanni, 'Responsible Digitalization through Digital Technologies and Green Practices', *Corporate Social Responsibility and Environmental Management*, Vol. 29, 2022, pp. 986–995, https://doi.org/10.1002/csr.2249.

Dong, Zhang, and Sana Ullah, 'Towards a Green Economy in China? Examining the Impact of the Internet of Things and Environmental Regulation on Green Growth', *Sustainability*, Vol. 15, No. 16, 2023, 12528, https://doi.org/10.3390/su151612528.

Edwards, Lilian, Derek McAuley, and Laurence Diver, 'From Privacy Impact Assessment to Social Impact Assessment', in *2016 IEEE Security and Privacy Workshops (SPW)*, IEEE, 2016, pp. 57–66, https://doi.org/10.1109/SPW.2016.19.

Ettari, Samantha V., 'Handling Internet of Things Data in Litigation', *E-Discovery Bulletin*, Kramer Levin

[17] Lilian Edwards, Derek McAuley and Laurence Diver, 'From Privacy Impact Assessment to Social Impact Assessment', in *2016 IEEE Security and Privacy Workshops (SPW)* (IEEE, 2016), 57 <https://doi.org/10.1109/SPW.2016.19>

Naftalis & Frankel LLP, December 2018/January 2019.

Julakanti, Sivananda Reddy, Naga Satya Kiranmayee Sattiraju, and Rajeswari Julakanti, 'Data Protection through Governance Frameworks', *Journal of Computational Analysis and Applications*, Vol. 31, No. 1, 2023, p. 158.

Lanfranchi, Giuseppe, Antonio Crupi, and Fabrizio Cesaroni, 'Internet of Things (IoT) and the Environmental Sustainability: A Literature Review and Recommendations for Future Research', *Corporate Social Responsibility and Environmental Management*, 2025, https://doi.org/10.1002/csr.2996.

Misra, S., et al., 'Green IoT: Energy Efficiency and Sustainable Smart Cities', *IEEE Communications Magazine*, Vol. 53, No. 1, 2015.

Pirson, J., and D. Bol, 'Assessing the Embodied Carbon Footprint of IoT Edge Devices Using Life-Cycle Assessment', *Journal of Cleaner Production*, Vol. 394, 2023.

Rathore, M., et al., 'Urban Planning and Smart City Decision Management Empowered by IoT', *Sustainable Cities and Society*, Vol. 32, 2017.

Shahriar, S., S. Allana, S. M. Hazratifard, and R. Dara, 'A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle', *IEEE Access*, Vol. 11, 2023, pp. 61831–61832, https://doi.org/10.1109/ACCESS.2023.3287195.

Sloot, Bart van der, Chris Jay Hoofnagle, and F. J. Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means', *Information & Communications Technology Law*, Vol. 28, No. 1, 2019, pp. 65–98, https://doi.org/10.1080/13600834.2019.1573501.

Taherdoost, Hamed, 'Security and Internet of Things: Benefits, Challenges, and Future Perspectives', *Electronics*, MDPI.