

Digital Creativity and Ethical Challenges: The Case of IoT in Creative Industries

Peng Lu Sen

City University Malaysia, 202105060103@student-city.edu.my

ABSTRACT

This paper aims to explore the ethical challenges emerging from the use of the Internet of Things (IoT) in the creative industries. As the application of IoT continues to grow, questions about data privacy, security, and intellectual property rights become paramount. By examining existing literature and industry examples, this paper presents a comprehensive overview of these ethical issues and suggests potential strategies for their mitigation.

Keywords: internet of things (IoT), creative industries, digital creativity, ethical implications, data privacy

I. INTRODUCTION

The digital revolution, driven by the exponential growth of technology, has reshaped the landscape of creative industries. One of the most transformative technologies at the forefront of this change is the Internet of Things (IoT). IoT, defined as a network of interconnected devices embedded with sensors, software, and network connectivity that enable data exchange and analysis, is driving unprecedented opportunities for creativity and innovation (Atzori, Iera, & Morabito, 2010). From wearable technology in fashion design to intelligent instruments in music production, IoT is redefining the boundaries of creativity, enabling artists and creators to explore new forms of expression (Belkhir & Elmeligi, 2020).

However, the integration of IoT into the creative process does not come without challenges. IoT's data-centric nature raises significant ethical issues, notably concerning data privacy, security, and intellectual property rights. The accumulation and analysis of large volumes of data often involve private, sensitive information, which can result in privacy violations if not properly managed (Ziegeldorf, Morchon, & Wehrle, 2014). Similarly, as creative processes become increasingly digitized, issues of copyright and intellectual property rights grow more complex (Schroff, 2017).

Moreover, the rapid pace of technological change can potentially widen the digital divide, reinforcing existing inequalities in access to technology and the ability to participate in creative industries (Van Dijk, 2017). This digital divide is not simply a matter of access but also includes disparities in digital literacy and the capacity to leverage IoT for creative pursuits (Hilbert, 2016).

This paper aims to explore these ethical implications of IoT in the creative industries and to initiate a discourse on potential strategies for addressing these challenges. This exploration is crucial in order to ensure a responsible, equitable, and sustainable growth trajectory for IoT-driven creativity.

II. LITERATURE REVIEW

A. Ethical Challenges in IoT-Driven Creative Industries

1) *Data Privacy and Security*

The surge of IoT devices in the creative industries introduces a new wave of data collection, bringing to light issues of data privacy and security. In their nature, IoT devices are built to generate, collect, and share data (Ziegeldorf, Morchon, & Wehrle, 2014). These data range from user interaction, location, behaviors, preferences, to more sensitive data like biometrics when it comes to wearable tech in the fashion industry. The granularity and the depth of this data collection could pose serious privacy risks.

Privacy issues are further intensified by the creative industry's inherent characteristics. Creators often have a deep relationship with their audience, which may involve sharing personal experiences, feelings, and thoughts (Hargittai & Marwick, 2016). IoT can facilitate such engagement but can also lead to inadvertent privacy breaches. For instance, an IoT-enabled performance may capture and share a performer's biometric data, blurring the lines between public and private spheres (Belkhir & Elmeligi, 2020).

Data security is another prominent concern. With the wide-scale integration of IoT, the creative industries are grappling with securing the immense volumes of data being generated (Roman, Zhou, & Lopez, 2013). IoT devices are often vulnerable to cyber threats due to their inherent interconnectedness and, in many cases, insufficient security measures. Data breaches could result in devastating effects, including unauthorized access to sensitive information and the potential for its misuse.

Moreover, the proliferation of IoT increases the potential for 'surveillance capitalism,' a term coined by Zuboff (2015) to describe the commodification of personal data. In this scenario, data collected by IoT devices could be used not only to tailor creative outputs to individual consumers but also to manipulate consumer behavior, raising ethical and privacy concerns.

2) *Intellectual Property Rights*

The integration of IoT technology within creative industries necessitates a re-evaluation of current intellectual property rights (IPR) frameworks. The nature of IoT blurs the boundaries of creation and innovation, as multiple entities, including IoT device manufacturers, software developers, and end-users, often contribute to a single

creative output (Schroff, 2017). This reality complicates traditional IPR paradigms, as it becomes challenging to identify who holds the rights to a creative work.

For instance, in the music industry, IoT technology like AI algorithms can assist in the composition process (Boden, Bryson, Caldwell, Dautenhahn, Edwards, Kember, Newman, Parry, Pegman, Rodden, Sorrell, Wallis, Whitby, & Winfield, 2017). Should these AI-assisted compositions be protected under copyright law? If so, who should be recognized as the rightful owner of the intellectual property, the algorithm's programmer, the user who engaged the AI, or the company that owns the AI software?

The proliferation of IoT in creative industries has also given rise to new forms of copying and unauthorized distribution. For example, 3D printing technologies can reproduce a physical object based on a digital model, challenging traditional notions of counterfeiting and piracy (Raustiala & Sprigman, 2019).

Furthermore, IoT devices often rely on open-source software, which poses additional intellectual property dilemmas. While the open-source approach fosters creativity and innovation, it can also be problematic for creators seeking to maintain exclusive control over their work (von Hippel & von Krogh, 2006).

Navigating the complex landscape of IPR in the age of IoT is therefore a pressing ethical challenge for the creative industries. As technology evolves, legal frameworks and ethical guidelines must be adapted to ensure fair and equitable practices, to protect the rights of creators, and to foster continued innovation.

3) *The Digital Divide*

The digital divide, referring to the inequality in access to, use of, or impact of information and communication technologies within a society (Hilbert, 2016), is a significant concern in the context of IoT in creative industries. The rapid pace of technological development, including the widespread integration of IoT, has the potential to widen this divide, thereby exacerbating social and economic inequalities.

While IoT technologies offer new platforms for creative expression and open up global markets for artists and creators, access to these technologies is uneven. It is often determined by a variety of factors, including socioeconomic status, geographical location, age, and education (Van Dijk, 2017). Consequently, these disparities can lead to unequal participation in the creative industries and can inhibit diversity and inclusivity in creative outputs.

Furthermore, the digital divide extends beyond physical access to technology; it also encompasses differences in digital literacy – the skills needed to use IoT technologies effectively (Hargittai, 2002). For example, to fully engage with IoT in creative industries, individuals need not only access to IoT devices but also skills in data analysis, network security, and digital rights management.

The ethical implications of the digital divide are significant. It raises questions about who can participate in IoT-enabled creative processes and whose voices and experiences are represented (and omitted) in creative outputs. It also highlights the role of creative industries in either perpetuating or challenging existing social inequalities. Addressing the digital divide in the context of IoT in creative industries, therefore, requires concerted

efforts from policymakers, educators, technology developers, and industry leaders. These efforts could include improving access to technology, investing in digital literacy education, and creating inclusive policies and practices that support diverse participation in creative industries.

B. Mitigation Strategies

1) *Creating Robust Security Measures*

The complexities of data privacy and security issues within the IoT-infused creative industries necessitate robust mitigation strategies to protect sensitive information and maintain users' trust (Ziegeldorf, Morchon, & Wehrle, 2014). To develop robust security measures, multiple fronts must be considered: technological solutions, regulatory frameworks, and user-awareness initiatives.

From a technological perspective, security in IoT systems can be enhanced through strong encryption methods, robust authentication mechanisms, and comprehensive system security architectures. Employing secure data encryption can protect sensitive data during transmission and storage, reducing the risk of unauthorized access or data breaches (Roman, Zhou, & Lopez, 2013). Multi-factor authentication methods, such as biometrics or tokens, can provide an additional layer of security, ensuring only authorized users can access the IoT devices and their data (Aldawood & Skinner, 2019).

However, technical measures alone cannot ensure absolute security and privacy. Regulatory frameworks play a crucial role in setting standards and enforcing responsible behavior among IoT stakeholders. Effective legislation needs to cover not only data protection and security requirements but also accountability and transparency standards. The European Union's General Data Protection Regulation (GDPR), for instance, has set comprehensive rules for data protection and includes strict penalties for non-compliance, thus representing a proactive step towards responsible data governance (Kuner, 2017).

Equally important is raising user awareness about privacy and security issues. User behaviors significantly impact the security of IoT systems, as users often represent the weakest link in the security chain (Wang, De, & Chaudhury, 2015). Therefore, educational programs aimed at improving digital literacy can play a key role in mitigating security risks.

The creative industries should also take a proactive stance in ensuring data security. Incorporating privacy-by-design principles, where privacy measures are embedded into the design of IoT systems from the outset, is one approach that could help mitigate potential data breaches (Cavoukian, 2010).

2) *Regulatory Framework*

Creating an effective regulatory framework is a critical component of addressing the ethical implications of IoT in the creative industries. A well-designed regulatory framework can provide clear guidelines for responsible behavior, ensure accountability, and protect individuals' rights (Schroff, 2017). Regulations such as the General Data Protection Regulation (GDPR) in the European Union offer a comprehensive set of rules regarding data protection and privacy. They also impose substantial penalties for non-compliance, therefore, promoting a

proactive approach towards data governance (Kuner, 2017). However, regulatory frameworks must be dynamic and adaptable, as the technology landscape and associated ethical challenges evolve continually.

Moreover, regulatory frameworks must extend beyond data privacy and security issues to address intellectual property rights and the digital divide. Laws and regulations should strive to protect creators' intellectual property rights in an environment where creation and innovation often involve multiple entities (Schroff, 2017). At the same time, policies should aim to reduce the digital divide by improving access to technology and investing in digital literacy education (Van Dijk, 2017). By focusing on these areas, regulatory frameworks can help ensure that the integration of IoT into the creative industries is carried out in an ethical, responsible, and equitable manner.

3) *Bridging the Digital Divide*

Mitigating the digital divide in the context of IoT in creative industries requires a multifaceted approach that goes beyond improving physical access to digital resources. As Hargittai (2002) suggests, strategies should also focus on developing digital literacy skills, which are critical for effectively utilizing and benefiting from IoT technologies. Public education initiatives, community outreach programs, and integrating digital literacy into school curriculums are potential approaches to enhance digital literacy levels across various demographics. Moreover, collaborations between educational institutions, government agencies, and tech companies can further amplify these efforts (Hilbert, 2016).

However, bridging the digital divide also necessitates addressing socioeconomic and geographical disparities in technology access. Policymakers must take action to provide affordable internet access and IoT devices in underprivileged areas. Incentives can be given to technology companies to develop affordable devices and services targeting these areas (Van Dijk, 2017). Moreover, the creative industries themselves must take a proactive role, perhaps through social responsibility programs, to ensure that their products, services, and platforms are accessible and inclusive. By adopting these strategies, we can progress towards a more equitable digital future in the creative industries powered by IoT.

III. CONCLUSION

In conclusion, the proliferation of IoT within creative industries presents a transformative opportunity, while also unearthing significant ethical implications. Critical issues such as data privacy and security, intellectual property rights, and the digital divide necessitate robust strategies to mitigate potential negative impacts. The resolution lies in adopting a multifaceted approach comprising technological advancements, regulatory frameworks, and efforts to bridge the digital divide. As the integration of IoT in creative industries continues to evolve, it is crucial to navigate this ethical landscape with a proactive and inclusive approach. Further interdisciplinary research is needed to explore these ethical challenges and potential solutions, ensuring that the benefits of IoT can be harnessed responsibly, equitably, and sustainably within the creative industries.

REFERENCES

- Aldawood, H., & Skinner, G. (2019). Security approaches for the Internet of Things: Protecting IoT environments from cyber threat. *Internet of Things*, 100137.
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805.
- Belkhir, L., & Elmeligi, A. (2020). Assessing the impact of the Internet of Things (IoT) on the sustainability of the creative industry. *Journal of Innovation and Entrepreneurship*, 9(1), 1-19.
- Boden, M., Bryson, J., Caldwell, D., Dautenhahn, K., Edwards, L., Kember, S., Newman, P., Parry, V., Pegman, G., Rodden, T., Sorrell, T., Wallis, M., Whitby, B., & Winfield, A. (2017). Principles of robotics: regulating robots in the real world. *Connection Science*, 29(2), 124-129.
- Bughin, J., Chui, M., & Manyika, J. (2015). Bridging the gap: Reaping the benefits of the IoT in the creative industry. *Digital McKinsey*, 23-29.
- Cavoukian, A. (2010). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.
- Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, 10, 21.
- Hilbert, M. (2016). The end justifies the definition: The manifold outlooks on the digital divide and their practical usefulness for policy-making. *Telecommunications Policy*, 40(6), 533-551.
- Kuner, C. (2017). The European Union's General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *Yale Journal of Law & Technology*, 19(1), 1-32.
- Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21.
- Raustiala, K., & Sprigman, C. (2019). The second digital disruption: Streaming & the dawn of data-driven creativity. *California Law Review*, 107, 1-33.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279.
- Schroff, S. (2017). Intellectual property rights and the ever-evolving internet. *Journal of Internet Law*, 21(3), 3-13.
- Van Dijk, J. A. (2017). Digital divide: Impact of access. In *The International Encyclopedia of Media Effects*. Wiley.
- Von Hippel, E., & von Krogh, G. (2006). Free revealing and the private-collective model for innovation incentives. *R&D Management*, 36(3), 295-306.
- Wang, P., De, S., & Chaudhury, A. (2015). A comprehensive survey on internet of things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, 2(3), 161-200.
- Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728-2742.
- Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89.