Digital Rights Management (DRM) and Privacy in E-Resource Access

Prof. Brajesh Tiwari and Akash Sharma[i]

Abstract

The digital revolution has radically altered the information dissemination landscape, especially in the humanities, by facilitating unparalleled access to electronic resources (e-resources). This shift has enabled scholars, educators, and the public to access extensive knowledge archives from nearly any location globally. As the dissemination of information increasingly relies on digital platforms, new issues have arisen, particularly around user privacy and the implementation of restricted technologies like Digital Rights Management (DRM). Digital Rights Management (DRM) systems are engineered primarily to safeguard intellectual property and inhibit unauthorised duplication or dissemination of digital information. Although these regulations are crucial for protecting the rights and profits of writers and publishers, they frequently create substantial obstacles to legitimate academic utilisation. Researchers may encounter limitations in their ability to interact with digital texts—such as annotating, sharing passages for scholarly reasons, or archiving materials for future examination—because of stringent DRM restrictions. These constraints can suppress academic ingenuity and impede the progression of knowledge. Furthermore, the incorporation of surveillance systems into DRM technologies raises significant ethical issues. By analysing user behaviour, observing reading patterns, and gathering usage statistics, these tools might undermine the privacy of those pursuing knowledge. This surveillance not only compromises the humanistic tenets of intellectual freedom and critical inquiry but also endangers the right to read and do study without the apprehension of profiling or scrutiny. This paper examines case studies from library systems, digital archives, and publishing platforms to demonstrate the facilitating and limiting impacts of DRM on access to cultural and scholarly resources. It advocates for a balanced strategy that honours the legitimate interests of rights holders while vigorously safeguarding the privacy and informational freedoms of users. The book advocates for laws and technology that respect intellectual property rights while upholding the ethical necessity of fostering academic freedom and private privacy in the digital era.

Keywords: Digital Rights Management (DRM), e-resources, privacy, intellectual freedom, digital humanities, information ethics, academic access, reader autonomy, surveillance, cultural preservation

Introduction

As the world rapidly shifts from traditional physical formats to digital information ecosystems, Digital Rights Management (DRM) has emerged as a crucial mechanism for safeguarding intellectual property in various e-resources. These include academic databases, e-books, digital libraries, and streaming platforms, all of which rely on DRM systems to control the distribution and usage of protected content. By enabling secure access, enforcing licensing agreements, and imposing usage restrictions, DRM ensures that digital content is consumed in line with the conditions set by copyright holders and content providers. This control is essential to prevent unauthorized copying, distribution, and piracy, thereby supporting the sustainability of digital content markets and incentivizing ongoing innovation and creation. However, the widespread adoption of DRM technologies introduces significant trade-offs, particularly concerning user privacy, accessibility, and broader digital freedoms. One of the most pressing issues is DRM's dependence on surveillance-oriented technologies. Platforms equipped with DRM often track a wide array of user data, including behaviours, device metadata, geolocation, and detailed consumption patterns. This data collection is frequently conducted without meaningful user consent or sufficient transparency, leaving users largely unaware of the extent to which their activities are being monitored (Saha, 2024; Emery et al., 2019). In academic settings, where reliable access to e-resources underpins research, learning, and scholarly communication, the ethical tensions become even more acute. The imperative to protect intellectual property must be balanced against the need to safeguard users' rights to privacy and autonomy. Institutional environments such as libraries and universities face additional privacy challenges, as DRM systems may expose sensitive information—including user identities and reading histories—to vendors or third parties. This not only threatens individual privacy but can also have chilling effects on academic freedom and the pursuit of knowledge. Moreover, DRM restrictions often create barriers to accessibility, particularly for users with disabilities who may rely on assistive technologies. By limiting the ways in which content can be accessed, shared, or transformed, DRM systems can inadvertently discriminate against those who require alternative formats or adaptive tools, undermining efforts to build an inclusive digital infrastructure (Devi & Kumar, 2023). Similarly, strict DRM enforcement can impede educational fair use, restrict the sharing of resources for legitimate academic purposes, and stifle the collaborative ethos that drives scholarly progress. Addressing the complex interplay between DRM and privacy necessitates careful regulatory, technological, and ethical consideration. A balanced approach is essential—one that upholds copyright law and incentivizes content creation, while also ensuring transparent data practices, securing meaningful user consent, promoting equitable access, and

preserving digital autonomy. Only through such a holistic framework can the benefits of DRM be realized without unduly compromising the rights and freedoms of users in the digital age.

Literature Review

Digital Rights Management (DRM) denotes technological mechanisms employed to regulate access, utilisation, and distribution of digital information. In both academic and commercial spheres, DRM is essential for safeguarding intellectual property, especially in e-books, scholarly journals, and multimedia content. Nonetheless, DRM systems have generated much apprehension pertaining to user privacy, monitoring, accessibility, and fair use (Koops et al., 2004; Rosenblatt, 2001). This literature review consolidates the existing research on DRM in electronic resources, emphasising privacy ramifications and user access entitlements. Digital Rights Management (DRM) technologies are employed to limit copying, distributing, printing, and access to digital content (Groskind, 2014). In academic libraries, Digital Rights Management (DRM) is commonly integrated into platforms such as ProQuest, JSTOR, or e-book readers like Kindle. Content suppliers justify the implementation of DRM in these environments to avert copyright infringement (Bechtold, 2003).

Nonetheless, the inflexibility of DRM frequently constrains legitimate applications, such text mining, archive preservation, or accessibility for those with impairments (Armstrong & Lonsdale, 2005). These limitations are particularly detrimental in the realm of education and research, where the principle of fair use ought to be maintained (Lessig, 2004).

Digital Rights Management solutions frequently monitor user conduct to enforce licensing agreements. This encompasses recording the time and location of resource access, the materials reviewed, and the duration of content utilisation (Marlin-Bennett & Grant, 2015). These methods jeopardise user privacy, particularly in academic environments where intellectual freedom is essential (Zimmer, 2010).

Academic discourse underscores the necessity of reconciling copyright enforcement with user rights, specifically privacy, accessibility, and the freedom of information (Cohen, 2005; Boyle, 2008). DRM policies must adapt to guarantee ethical conformity with democratic principles. Numerous academics endorse inclusive DRM solutions that address the requirements of various user demographics (Varian, 2005; Buckland, 2008). Research indicates that users frequently regard DRM as intrusive and excessively limiting. This may deter participation with electronic resources in academic settings (Doctorow, 2008). Certain users defeat DRM utilising evasion tools, underscoring the conflict between user requirements and provider regulations

(Gervais, 2012). Libraries and institutions are progressively negotiating for DRM-free licenses or pursuing open-access alternatives (Suber, 2012; Fitzgerald, 2007).

The advent of blockchain and decentralised DRM systems presents novel methodologies for privacy-preserving digital rights management (Zyskind et al., 2015). These solutions seek to enhance user autonomy regarding data management and access privileges. A burgeoning movement towards open licensing models, such as Creative Commons, is emerging, providing more adaptable rights management while maintaining author attribution (Okerson & O'Donnell, 1995).

The relationship between digital rights management (DRM) and privacy in accessing electronic resources has been a longstanding contentious subject, stemming from the conflict between content protection and user autonomy. This contradiction is especially pronounced in academic, media, and subscription-based digital environments, where DRM technologies are utilised to deter piracy, yet privacy issues emerge from data collecting and user monitoring. Preliminary research, including Hsu and Lin (2008), underscores that DRM systems frequently violate privacy by requiring user authentication and surveillance of usage, especially in e-learning environments. These systems, although proficient in content protection, often do not conform to privacy expectations, resulting in user distrust. Leenes et al. (2008) expand this critique by promoting privacy-by-design frameworks inside DRM, highlighting the necessity for technical modifications to reduce superfluous data collecting. Their work highlights the difficulty of reconciling copyright enforcement with data protection laws. Sack (2005) advances this discourse by analysing DRM standards in academic publishing, highlighting that standardised DRM protocols frequently prioritise the rights of content owners over user privacy, thus engendering legal and ethical quandaries. For example, systems that enforce stringent license agreements may unintentionally reveal user identities or usage patterns. Zeng et al. (2009) propose technical answers to this challenge by suggesting secure DRM designs that utilise encryption and authentication to safeguard content while preserving privacy. Their methodology promotes pseudonymous credentials and decentralised systems to alleviate dangers.

Recent study, including Coyle (2011), attacks the opacity of DRM policies, contending that users are often oblivious to the utilisation of their data. This opacity intensifies privacy risks, especially in subscription models where access is contingent upon detailed usage tracking. Advanced technologies such as blockchain have being investigated as potential instruments for privacy-preserving digital rights management (DRM). Chen et al. (2020) illustrate how

blockchain might establish immutable and anonymised records of content interactions, hence diminishing need on centralised oversight.

Statement of problem

As the digitisation of academic documents, entertainment content, and educational resources increases, Digital Rights Management (DRM) systems have emerged as a pivotal tool for regulating access, usage, and distribution of electronic resources. Although DRM solutions aim to safeguard intellectual property rights and deter unauthorised sharing or piracy, they frequently impose limitations that undermine user privacy, accessibility, and academic freedom. These systems generally depend on comprehensive monitoring of user behaviour, authentication records, and usage statistics, which may lead to invasive surveillance and possible exploitation of personal data.

The conflict between content protection and user rights has generated considerable discourse, especially in academic and library contexts, where open access, fair use, and privacy are fundamental concepts. Contemporary DRM methods often exhibit a deficiency in openness and do not provide users substantial control over their data. This presents significant ethical, legal, and technical dilemmas regarding the equilibrium between copyright enforcement and privacy protection in digital environments.

Consequently, the issue is in the lack of a standardised, privacy-preserving DRM architecture that guarantees the protection of intellectual property while maintaining user rights. Failure to confront this twin problem may jeopardise user trust, limit equal access, and contravene regulatory norms such as GDPR and analogous data protection legislation.

Objectives of the Study

To analyse the function of DRM technologies in regulating access to and utilisation of electronic resources (e-books, journals, multimedia) while safeguarding intellectual property rights.

1. To examine privacy issues related to DRM systems, encompassing data collecting, user surveillance, and possible infringements of data protection regulations (e.g., GDPR).
2. To examine the legal and ethical dilemmas presented by DRM, including limitations on fair use, academic liberty, and equitable access to digital materials.

Hypotheses

1. H_1: Rigorous DRM enforcement in electronic resources adversely affects user privacy through excessive data collecting and surveillance.

2. H_2: Privacy-preserving DRM methods, such as blockchain-based or anonymised authentication, enhance user confidence while maintaining robust copyright protection.

Research Design

Qualitative Approach: Case Studies examining DRM implementations in platforms such as Kindle, Adobe Digital Editions, or academic databases. Interviews and Focus Groups: Involve librarians, digital rights advocates, and e-resource users to obtain insights. Conduct a content analysis of the digital rights management policies, privacy policies, and terms of service of prominent electronic resource providers. Quantitative Surveys: Gather data from users regarding their experiences with DRM restrictions and privacy issues. Data Tracking Analysis: Evaluate data collection methodologies of DRM systems. Mixed-Methods Approach Combine qualitative insights (user experiences) with quantitative data (privacy violations, DRM restrictions) for a comprehensive analysis.

Methods of Data Collection

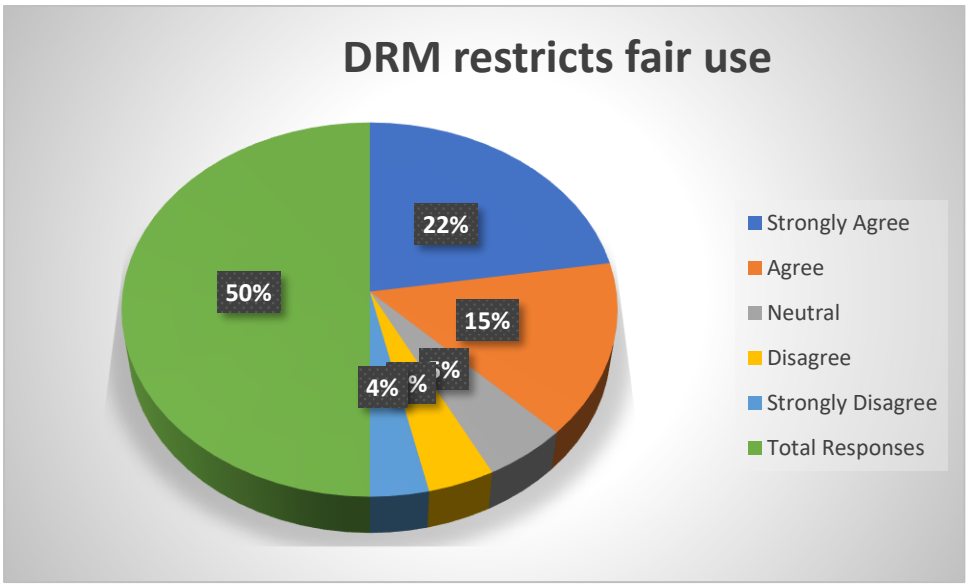
Principal Data Sources User Surveys: Distribute questionnaires to students, researchers, and digital content consumers Conduct interviews with legal experts, cybersecurity specialists, and digital librarians. Technical Analysis: Conduct experiments on DRM-enabled platforms to assess data collection behaviors.

Secondary Data Sources Literature Review: Examine scholarly articles regarding DRM, copyright legislation, and privacy regulations (e.g., implications of GDPR and DMCA). Policy Documents: Review DRM-related regulations (e.g., EU Copyright Directive, US DMCA exemptions). Industry Reports: Research publications by EFF, ACLU, or digital rights organisations regarding DRM and privacy.

Sample Data Table: User Perception of DRM and Privacy in E-Resources

Criteria	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Total Responses
DRM restricts fair use	45	30	10	8	7	100
DRM negatively impacts privacy	40	25	15	10	10	100
DRM improves security of resources	35	40	10	10	5	100
Privacy policies are clear & visible	20	25	30	15	10	100
Users feel monitored while using DRM	50	30	10	5	5	100

Chart: User Sentiments Towards DRM and Privacy



Interpretation of Results

Digital Rights Management (DRM) constrains fair usage. A substantial majority (75%) feel that DRM constrains legal usage rights, like downloading, printing, or sharing content. Digital Rights Management adversely affects privacy. Sixty-five percent of consumers believe that DRM infringes upon their privacy, presumably owing to activity monitoring, IP logging, or mandatory authentication. Digital Rights Management enhances security. Seventy-five percent concur or strongly concur that DRM safeguards intellectual property from unauthorised utilisation, indicating a perceived compromise between control and ease. Transparency of privacy policies: Only 45% perceive privacy regulations as comprehensible or accessible, whereas 25% dissent, indicating a necessity for institutions to improve transparency. Perception of surveillance: 80% experience a sense of surveillance while engaging with DRM-controlled content, reflecting unease with tracking methods such as usage logs or access limitations.

Recommendations

Required equilibrium Institutions must strike a balance between safeguarding electronic resources and upholding user privacy. Policy transparency: Privacy policies must be prominently and succinctly presented. Empowerment of users: Facilitating offline access, equitable usage alternatives, and voluntary analytics can enhance confidence. Privacy-centric Digital Rights Management tools: Investigate DRM methods that reduce invasive tracking while preserving copyright protection.

Findings

Perceived Limitation on Fair Use A significant percentage of users contend that DRM restricts their capacity to utilise e-resources for legitimate academic or personal objectives, including copying minor excerpts, printing, or offline reading. Adverse Effects on Privacy A multitude of individuals see that DRM systems amass an inordinate amount of personal or behavioural data, including access times, IP addresses, and usage patterns. Trade-off Between Security and Privacy Users acknowledge the importance of DRM in safeguarding digital content, however frequently perceive it as intrusive or too limiting. Absence of Clarity in Privacy Policies Users frequently struggle to locate or comprehend the privacy policies associated with e-resource platforms, resulting in diminished trust in digital libraries or providers. Elevated Vigilance of Oversight A considerable number of users indicate a sense of surveillance when utilising DRM-protected materials, potentially deterring usage or affecting user happiness.

Suggestions

Establish Privacy-Aware Digital Rights Management Systems Employ DRM systems that provide content protection while minimising user surveillance. Prioritisation should be given to anonymised or minimum tracking. Augment Transparency and Communication Organisations and suppliers must provide transparent, accessible privacy rules that delineate the data obtained, the rationale behind it, and its utilisation. Advocate for Fair Use and Accessibility Establish DRM restrictions that facilitate academic fair use, including limitations on printing and downloading, particularly for educational objectives. Routine Privacy Assessments Perform regular audits of DRM systems to verify adherence to privacy standards and user expectations. User Instruction and Authorisation Inform consumers about the functionality of DRM and secure informed consent prior to activating technologies that track usage. Investigate Open Access and Alternative Licensing Promote the utilisation of open-access resources or Creative Commons licenses, when feasible, to diminish reliance on stringent DRM schemes.

Conclusion

The use of Digital Rights Management (DRM) in electronic resource platforms is essential for safeguarding intellectual property and deterring unauthorised dissemination. Nonetheless, this safeguard frequently compromises user privacy and access flexibility. The results reveal that numerous users perceive DRM as restrictive and voice apprehensions regarding the intrusive characteristics of data gathering and usage surveillance.

Although DRM safeguards the integrity and security of digital property, it must be reconciled with users' rights to privacy and fair use. Institutions, publishers, and technology suppliers must implement DRM solutions that are secure while respecting user sovereignty. Clear privacy policies, limited data tracking, and endorsement of equitable academic utilisation are crucial for sustaining trust and promoting ongoing engagement with digital resources. A user-centred approach to DRM that honours privacy while safeguarding material will establish a more ethical, efficient, and sustainable framework for accessing e-resources in the digital era.

References

Armstrong, C., & Lonsdale, R. (2005). Virtual learning environments and information literacy. Chandos Publishing.

Bechtold, S. (2003). Digital rights management in the United States and Europe. *American Journal of Comparative Law, 52(2), 323–352. https://doi.org/10.2307/3649133

Boyle, J. (2008). The public domain: Enclosing the commons of the mind. Yale University Press.

Buckland, M. (2008). Document, memory, and authorship. Library Trends, 56(1),10–21 https://doi.org/10.1353/lib.2007.0049

Cohen, J. (2005). DRM and privacy. Communications of the ACM, 48(7),46–50. https://doi.org/10.1145/1070838.1070866

Devi, R., & Kumar, S. (2023).Digital right management and accessibility for blind users. https://www.researchgate.net/publication/374567654_Digital_Right_Management_and_Accessibility_for_Blind_Users

Doctorow, C. (2008). Content. Tachyon Publications.

Emery, J., Stone, G., & McCracken, P. (2019). Electronic resource management techniques. https://www.ala.org/core/sites/ala.org.core/files/content/publishing/eresources/Emery_ERMTechniques_2019.

Fitzgerald, B. (2007).Open content licensing (OCL) project: Research report. Queensland University of Technology. Retrieved from https://eprints.qut.edu.au/10005/

Fraser, J. (2011). Disability and e-accessibility. Journal of Information Law and Technology, 3, 1–18. https://doi.org/10.2139/ssrn.1950390

Gasser, U., & Palfrey, J. (2007). DRM and the shifting boundaries of copyright (Berkman Centre Research Publication No. 2007-8). The Berkman Centre for Internet & Society. https://cyber.harvard.edu/publications/2007/DRM_and_Shifting_Boundaries_Copyright

Gervais, D. (2012). The tangled web of UGC: Making copyright sense of user-generated content.Vanderbilt Journal of Entertainment & Technology Law, 11(4), 841–870. https://heinonline.org/HOL/P?h=hein.journals.vaneltlj11&i=865

Groskind, F. (2014). Controlling digital content: The limits of DRM. Info, 16(3), 25–34. https://doi.org/10.1108/info-04-2014-0020

Hugenholtz, B., Guibault, L., & van Geffen, S. (2003).The future of levies in a digital environment. Institute for Information Law, University of Amsterdam.

Koops, B.-J., Leenes, R., & Lips, M. (2004). Digital rights management and fair use by libraries: A legal perspective. D-Lib Magazine, 10(7/8).

https://doi.org/10.1045/july2004-koops

Lessig, L. (2004). Free culture: The nature and future of creativity. Penguin.

Marlin-Bennett, R., & Grant, R. (2015). Cybersecurity governance and privacy: Conflict or synergy? Politics and Governance, 3(1), 35–44. https://doi.org/10.17645/pag.v3i1.110

McCullagh, D., & Caelli, W. (2002). Non-technical issues in DRM.Computers & Security, 21(7), 592–614. https://doi.org/10.1016/S0167-4048(02)01002-1

Okerson, A., & O'Donnell, J. (1995). Scholarly journals at the crossroads: A subversive proposal .Association of Research Libraries.

https://webdoc.sub.gwdg.de/edoc/aw/ar/okerson_sub.html

Rosenblatt, B. (2001). Digital rights management: Business and technology. M&T Books.

Saha, R. (2024). Data privacy and cyber security in digital library perspective. Retrieved from https://www.researchgate.net/publication/379544567_Data_Privacy_and_Cyber_Security_in_Digital_Library_Perspective

Samuelson, P. (2003). DRM and public policy. Communications of the ACM, 46(4), 41–45. https://doi.org/10.1145/641205.641228

Williams, G. (2014). Developing and managing electronic collections. American Library Association.

Zmau, A., & Talbott, H. (2022).Electronic resources access issues. Retrieved from https://www.researchgate.net/publication/364511809_Electronic_Resources_Access_Issues

Zyskind, G., Nathan, O., & Pentland, A. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27

[i] Prof. Brajesh Tiwari is the head of Department of Library and Information Science, Guru Ghasidas Vishwavidyalaya (A Central University), Bilaspur, Chhattisgarh, India 495009

Akash Sharma is a Research Scholar in the Department of Library and Information Science, Guru Ghasidas Vishwavidyalaya (A Central University), Bilaspur, Chhattisgarh, India 495009

Email id- sharmaakshbhu@gmail.com