Journal of Media and Communication

[ISSN 2958-1095]
Volume: 05 Issue: 01 | January-2026

JMC

The Contribution of Multimedia Technologies to the Sharing of Employee Personal Information in Public Institutions

Authors

Alfred Misheba [1]; James Ogalo [2]; Jonai Wabwire [3]

Main author's email: Mishebalfred@gmail.com

(1.2.3) Kisii University, Kenya.

Cite this article in APA

Misheba, A., Ogalo, J., & Wabwire, J. (2026). The contribution of multimedia technologies to the sharing of employee personal information in public institutions. *Journal of media and communication*, 5(1), 01-07. https://doi.org/10.51317/jmc.v5i1.882

OPEN ACCESS

A publication of Editon Consortium Publishing (online)

Article history

Received: 2025-11-13
Accepted: 2025-12-9
Published: 2026-01-12

Scan this QR to read the paper online

Abstract

This study investigates how multimedia technologies enhance the creation, sharing, and exposure of employee personal information in public institutions. Widespread use of smartphones, social media platforms, cloud-based communication systems, and video-conferencing tools increasingly exposes sensitive employee personal information. The study is conducted within the scope of Kisii County Government in Kisii County, Kenya, using a descriptive case study design. Data were collected from a total of 131 participants, comprising employees drawn from the Communication (30), Information Technology (40), and Human Resource Management (47) departments, as well as 14 chief officers selected through purposive sampling. The findings reveal that multimedia technologies accelerate the generation, storage, circulation, and public sharing of employee personal information. Employees frequently expose sensitive information unintentionally through social media sharing, misconfigured cloud access, and video conferencing errors. While these technologies enhance communication efficiency and organisational collaboration, they simultaneously reduce employee control over personal data, creating persistent privacy vulnerabilities within public institutions. The study concludes that employee privacy risks are shaped by both individual practices and institutional frameworks, and recommends strengthening digital privacy governance through comprehensive privacy policies, continuous privacy awareness training, secure cloud systems, automated privacy safeguards, and clear social media usage guidelines.

Key terms: Cloud computing, digital privacy, employee-created content, multimedia technologies, public institutions, social media.

INTRODUCTION

The rapid adoption of multimedia technologies has transformed communication and information management within public institutions, enhancing operational efficiency but also introducing significant risks to employee privacy (Smith et al., 2011). The integration of digital platforms enables unintended creation, sharing, and circulation of employee-generated content, which can expose sensitive personal information to unauthorised access and weaken individual control over private data (Culnan & Bies, 2003; Dinev & Hart, 2005). This problem is especially acute in public sector settings where digital governance frameworks may be underdeveloped.

In the context of Kenya, and particularly within Kisii County Government, where digital communication tools are increasingly embedded into administrative operations and service delivery, employees generate a wide array of digital content: messages, documents, images, videos, and social media posts, using both official and personal devices (Kesan & Hayes, 2012; Westin, 2003). The instantaneous, cross-platform nature of multimedia technologies amplifies the risk that this content may be disclosed beyond intended audiences (Bélanger & Crossler, 2011). Organisational structures in public institutions characterised by broad internal data access, hierarchical communication norms, and limited privacy controls further deepen these risks, especially when platforms are used for both professional and personal purposes (Nissenbaum, 2010; Li et al., 2016).

Although workplace privacy has been widely studied, existing research largely focuses on private sector contexts or global perspectives, with limited empirical examination of how multimedia technologies affect employee privacy in public institutions in developing countries. Such gaps include insufficient exploration of institutional governance mechanisms, regulatory environments, and behavioural drivers that shape privacy exposure in these settings.

Against this backdrop, this study investigates how multimedia technologies such as cloud services, instant messaging, social media platforms, and video conferencing facilitate the creation, sharing, and dissemination of employee personal information within public institutions. It also examines how institutional weaknesses, including inadequate privacy policies and limited employee awareness, amplify the exposure and uncontrolled circulation of sensitive information. These insights lay the foundation for a detailed analysis of the mechanisms, risks, and governance factors influencing employee privacy in the digital workplace.

LITERATURE REVIEW

Overview of Multimedia Technologies and Workplace Communication

Multimedia technologies integrate text, images, audio, and video within interconnected digital platforms, reshaping how organisations communicate and manage information (Ellison et al., 2007). Early scholarship largely frames these technologies as efficiency-enhancing tools that support communication, document management, data storage, and collaboration (Zhou, 2011). From this perspective, speed, connectivity, and ease of duplication are viewed as functional advantages that improve organisational coordination.

However, privacy-focused research presents a contrasting interpretation. Culnan and Bies (2003) and Dinev and Hart (2005) argue that the same features enabling efficiency simultaneously weaken employee control over personal information by facilitating rapid replication, forwarding, and storage of digital content. This tension illustrates a key convergence in the literature. Scholars agree that multimedia technologies are indispensable to modern workplaces, yet they diverge on whether their benefits outweigh the privacy risks they introduce.

In public institutions, this duality is particularly pronounced. Multimedia tools support official correspondence, record management, online meetings, and public engagement, but operate within bureaucratic systems characterised by hierarchical authority, shared access privileges, and heightened transparency requirements. While cloud services and instant messaging platforms enhance interdepartmental collaboration, they also expand access points to sensitive information, increasing the likelihood of unintended disclosure through misconfigured permissions and persistent access (Li et al., 2016). Video-conferencing systems similarly enable real-time collaboration but capture audio-visual data

that may expose private environments, especially in remote work contexts (Marx, 2016). Existing studies thus converge on the centrality of multimedia technologies in public sector communication but diverge in their assessment of how effectively public institutions manage the accompanying privacy risks. Table 1 contextualises workplace privacy risks by linking specific technologies to both workplace use and associated privacy concerns.

Table 1: Multimedia Technologies and Workplace Functions

Technology	Workplace Use	Privacy Concerns
Cloud Services	Data storage, remote access	Persistent data, misconfigured access
Instant Messaging	Real-time departmental communication	Accidental forwarding, wrong recipient
Social Media	Sharing events, engagement	Unintended visibility, tagging issues
Video Conferencing	Meetings, document collaboration	Screen-sharing errors, visual exposure

Employee-Created Content and Digital Privacy

Employee-created digital content, including emails, messages, documents, images, recordings, and social media posts, is a major source of workplace privacy exposure (Kesan & Hayes, 2012). Digital privacy scholarship defines privacy as employees' ability to control how their personal information is collected, used, and shared (Nissenbaum, 2010). Yet, research increasingly suggests that such control is undermined by constant connectivity, cross-platform integration, and automated data synchronisation (Dinev & Hart, 2005).

Studies converge in identifying routine workplace practices such as accidental forwarding, screen sharing errors, password sharing, and uncontrolled cloud access as primary causes of privacy breaches rather than external cyberattacks (Westin, 2003). However, more recent interpretations emphasise that these exposures are not merely individual mistakes but are embedded within platform design and institutional norms that normalise constant sharing. This shift highlights a divergence in the literature between individual-centric explanations of privacyloss and systemic, technology-driven accounts of exposure.

Table 2 illustrates the range of content types generated by employees and the distinct privacy risks associated with each.

Table 2: Employee-Created Digital Content

Content Type	Examples	Potential Privacy Risk
Emails	Internal/external messages	Accidental forwarding, exposure
Documents/Reports	Reports, memos	Unauthorised access, long-term storage
Images/Videos	Photos of workplace/home events	Revealing personal/private information
Recordings	Audio/video recordings	Sensitive discussions captured
Social media posts	Workplace updates, personal posts	Sharing beyond the intended audience
Screenshots	Captured screens	Preserving confidential information

Table 3 highlights routine workplace practices that frequently lead to privacy breaches. The findings demonstrate that privacy risks largely arise from everyday employee actions rather than malicious intent.

Table 3: Routine Practices Leading to Privacy Breaches

Routine Practice	Description	Risk Mechanism
Accidental forwarding	Sending info to the wrong recipient	Unintended exposure
Screen capturing	Taking screenshots	Permanent record of sensitive info
Sharing passwords	Password reuse or sharing	Unauthorised access
Uncontrolled cloud sharing	Open/shared folders	Extended access beyond the intended audience

Smartphones, Social Media, and Privacy Exposure

Smartphones intensify privacy risks by consolidating multiple communication and storage functions into a single device used for both professional and personal activities (Ellison et al., 2007). While early research emphasised their productivity benefits, later studies show that this convergence blurs boundaries between work and private life, increasing the likelihood of inadvertent disclosure (Li et al., 2016). Social media platforms further amplify these risks through tagging, reposting, algorithmic distribution, and digital permanence, rendering privacy settings insufficient safeguards (Bélanger & Crossler, 2011).

Cloud Systems and Digital Permanence

Cloud-based systems improve efficiency through shared drives and collaborative documents but introduce persistent privacy risks due to indefinite data retention and complex access controls (Marx, 2016). Unlike earlier concerns centred on external threats, contemporary research emphasises internal governance failures, outdated permissions, weak audits, and unclear accountability as major sources of unauthorised access in public institutions (Culnan & Bies, 2003). This literature increasingly converges on the view that privacy risks are shaped less by technology itself than by institutional governance structures.

Video Conferencing and Visual Privacy

Video conferencing technologies pose significant privacy risks. They record visual and audio data, which can expose employees' homes, family members, personal belongings, and private conversations during meetings (Marx, 2016).

Once employee-created content is uploaded to cloud servers, it can remain accessible even after deletion from personal devices. Misconfigured permissions, shared links, and outdated access rights may allow unauthorised access. Because cloud-stored data is persistent, a single privacy breach can have long-lasting consequences (Culnan & Bies, 2003).

Theoretical Perspectives

Communication Privacy Management Theory

Communication Privacy Management Theory explains how individuals control the flow of private and public information. People set rules about what to share, with whom, and under which conditions (Petronio, 2002, as cited in Bélanger & Crossler, 2011). Once shared, private information becomes collectively controlled rather than solely individual. In digital workplaces, multimedia technologies weaken these boundaries by allowing instant replication and redistribution of private content.

Technological Determinism

Technological Determinism Theory proposes that technology drives social behaviour (Smith et al., 2011). Multimedia technologies influence employee communication by promoting constant sharing, instant documentation, and visual expression. As a result, privacy risks emerge not from deliberate actions but from behaviours normalised by the widespread use of these technologies.

Uses and Gratifications Theory

Uses and Gratifications Theory explains that employees adopt multimedia tools for convenience, speed, entertainment, efficiency, and social connection (Zhou, 2011). However, these motivations often override attention to privacy, causing employees to unintentionally expose private content.

Gaps in Existing Research

Although numerous studies examine digital privacy, several gaps remain: Limited focus on employee-

created content rather than institutional data (Kesan & Hayes, 2012), Minimal research on public institutions in developing countries (Marx, 2016), Little emphasis on accidental and behavioural privacy exposure (Culnan & Bies, 2003), and Weak integration of multimedia convergence and employee privacy risks (Bélanger & Crossler, 2011)

This study directly addresses these gaps by investigating how multimedia technologies drive the creation, transmission, and exposure of employee-created private content, providing empirical insight into a previously underexplored aspect of digital privacy in public institutions.

METHODOLOGY

This study adopted a descriptive case study design to investigate how media convergence shapes employee privacy practices within Kisii County Government, a public-sector institution experiencing extensive multimedia integration in workplace communication (Yin, 2014). The approach enabled an in-depth examination of real-life contextual dynamics. The target population included employees from the Communication, ICT, and Human Resource departments, which handle content creation, data management, and digital interactions. Data were collected from 117 employees via structured questionnaires (30 from Communication, 40 from ICT, and 47 from Human Resources). In addition, 14 chief officers were purposively selected as key informants for semi-structured interviews due to their policy and managerial roles.

Sampling combined purposive and simple random techniques. Departments and senior officers were purposively chosen for their direct relevance to media convergence and governance. Within departments, simple random sampling selected questionnaire respondents to ensure equal selection probability and minimise bias. Two instruments were used: structured questionnaires with closed-ended items assessing multimedia technology use, employee-created content, and privacy exposure; and semi-structured interview guides exploring perceptions of privacy risks, institutional controls, and governance practices. Validity was ensured through expert review, literature alignment, and a pilot study for item refinement. Reliability was checked via internal consistency.Quantitative data were analysed using descriptive statistics (frequencies and percentages)to reveal patterns in technology adoption and privacy incidents. Qualitative interview data underwent thematic analysis, involving familiarisation, coding, categorisation, and theme development to identify recurring behavioural and organisational patterns. Ethical clearance was obtained beforehand. Participants were informed of the study purpose, assured of anonymity and confidentiality, and provided written informed consent; participation remained voluntary.

RESULTS AND DISCUSSION

Contribution of Multimedia Technologies to Private Content Sharing

The findings indicate that multimedia technologies significantly accelerate the creation and circulation of employee personal information within Kisii County Government.

A large proportion of respondents (78%) reported using smartphones as their primary work device, with 71 per cent indicating that the same device was used simultaneously for both personal and official communication. This overlap increased the likelihood of unintentional content sharing. One respondent noted:

"Sometimes personal photos or messages mix with work files because everything is on one phone."

Social media platforms emerged as major channels of unintended privacy exposure. 64 per cent of respondents acknowledged having shared workplace-related content on social media platforms, while 42 per cent reported that such content later circulated beyond the intended audience. Interview data revealed limited awareness of how reposting, tagging, and screenshots extend content visibility. A senior officer stated:

"Once something is shared online, even in a closed group, it becomes difficult to control where it ends up."

Cloud-based systems also contributed to privacy exposure. 58 per cent of respondents reported storing work-related documents on shared cloud folders, and

37 per cent indicated that they were unsure who could access those files. Notably, 29 per cent confirmed awareness of instances where former employees retained access to shared folders after role changes or transfers.

Video conferencing tools presented additional risks. 46 per cent of respondents reported accidental exposure during virtual meetings, including unintended screen sharing and visibility of private home environments. One interview participant explained:

"Sometimes you forget what is open on your screen, and everyone sees it."

The findings demonstrate that routine use of multimedia technologies exposes employee-created content to unintended audiences through everyday communication practices rather than deliberate misuse.

Discussion

The results demonstrate that media convergence significantly weakens employee control over private information by collapsing the boundaries between personal and professional communication spaces. Consistent with Communication Privacy Management Theory, once private content enters shared digital systems, control shifts from the individual to multiple stakeholders, increasing the risk of exposure.

The dominance of smartphones and cloud platforms illustrates technological determinism, where employee behaviour adapts to the logic of speed, convenience, and constant connectivity. Privacy exposure thus becomes a structural outcome of digital work environments rather than isolated user error.

The findings highlight unique challenges within public-sector institutions, where shared platforms, broad access privileges, and weak access audits intensify privacy risks. These institutional characteristics amplify the permanence and reach of employee-created digital content, reinforcing the need for governance-oriented privacy interventions.

CONCLUSION AND RECOMMENDATIONS

Conclusion: The study establishes that multimedia technologies play a central role in facilitating the creation, storage, and circulation of employee personal information within public institutions. Smartphones, social media platforms, cloud systems, and video conferencing tools enhance communication efficiency while simultaneously increasing vulnerability to privacy exposure. The convergence of personal and professional communication, combined with persistent digital storage and shared access systems, significantly undermines employee privacy control.

Recommendations: Public institutions should strengthen digital privacy governance by enforcing clear multimedia use policies and conducting regular access audits for cloud-based systems. Mandatory employee training on digital privacy risks should be institutionalised to promote responsible content creation and sharing. Video conferencing platforms should implement stricter default privacy controls, including restricted screen sharing and secure recording management. Additionally, clear social media conduct guidelines should be enforced to minimise unintended disclosure of employee personal information.

Limitations: The study was limited to a single county government institution, which may affect the generalisability of the findings.

REFERENCES

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, 35(4), 1017–1041. https://doi.org/10.2307/41409971

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59(2), 323–342. https://doi.org/10.1111/1540-4560.00067

Dinev, T., & Hart, P. (2005). Internet privacy concerns and their antecedents—Measurement validity and a regression model. Behaviour & Information Technology, 24(1), 1–14. https://doi.org/10.1080/01449290410001715723

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Kesan, J. P., & Hayes, C. M. (2012). Mitigative counterstriking: Self-defence and deterrence in cyberspace. Harvard Journal of Law & Technology, 25(2), 429–476.

Li, H., Sarathy, R., & Zhang, X. (2016). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. Decision Support Systems, 91, 1–13. https://doi.org/10.1016/j.dss.2016.07.004

Marx, G. T. (2016). Windows into the soul: Surveillance and society in an age of high technology. University of Chicago Press.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. State University of New York Press.

Smith, M. L., Noorman, M., & Martin, A. K. (2011). Accountabilities, automation, and surveillance: The politics of information technologies. Surveillance & Society, 8(4), 355–368. https://doi.org/10.24908/ss.v8i4.4185

Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Yin, R. K. (2014). Case study research: Design and methods (5th ed.). Sage Publications.

Zhou, T. (2011). Understanding online community user participation: A social influence perspective. Internet Research, 21(1), 67–81. https://doi.org/10.1108/10662241111104884