International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com

Original Article

Data Privacy in Local Government Units: A Moor's Theory of Privacy Approach

Kimberly D. Degala[1], Anne M. Villanueva[2], Jonel P. Lañada[3]

Author Information:
[1-3]College of Arts and Science, West Visayas State University, Ilo-Ilo, Philippines

Correspondence: kaddegala@gmail.com

Article History:

Date Received: May 13, 2026
Date Revised: May 21, 2026
Date Accepted: June 11, 2026
Date Published: October 13, 2026

DOI: https://doi.org/10.67903/ijroms0111

Document ID: *2026IJROMS0111*

Recommended Citation:
Degala, K. D., Villanueva A. M. & Lañada, J. P. (2026). Data Privacy in Local Government Units: A Moor's Theory of Privacy Approach. International Journal of Research on Multidisciplinary Studies, 1(9), 290–296. https://doi.org/10.67903/ijroms0111

Abstract. This study investigates the awareness and implementation of the Data Privacy Act of 2012 (RA 10173) among Local Government Unit (LGU) employees through the lens of James Moor's Comprehensive Theory of Privacy. Using a quantitative, descriptive-correlational design, 78 randomly selected LGU personnel were surveyed to assess their level of awareness, extent of implementation, and associations with demographic factors, including sex, educational attainment, and employment status. Results indicate that employees demonstrate high awareness, while implementation is largely applied, with no significant differences across demographic groups. This suggests that organizational culture, institutional policies, and shared ethical responsibility exert a greater influence on privacy practices than individual characteristics. A strong positive relationship between awareness and implementation highlights knowledge as a moral and practical foundation for ethical data handling. The study underscores Moor's Restricted Access/Limited Control (RALC) framework, emphasizing that privacy is context-dependent, ethically grounded, and institutionally mediated. Recommendations include continuous training, clearly articulated privacy policies, monitoring mechanisms, and fostering a culture of ethical accountability to enhance data privacy compliance in LGUs.

Keywords: Data Privacy Act; Moor's Theory of Privacy; Local Government Units

Introduction

The disclosure of relevant and sensitive information must be treated with utmost care and confidentiality, particularly in the digital age where technological advancements have significantly increased the generation, storage, and transmission of personal data (Olsson, 2019; Dizon, 2018). The rapid digitalization of institutional processes has intensified concerns regarding data privacy and information security, prompting governments worldwide to establish regulatory mechanisms to safeguard personal information. In the Philippines, the enactment of Republic Act No. 10173, otherwise known as the Data Privacy Act (DPA) of 2012, represents a major legislative initiative aimed at regulating the collection, processing, storage, and use of personal data. The law seeks to protect individuals' right to privacy while allowing the legitimate flow of information. The Act was signed into law on August 15, 2012, and its Implementing Rules and Regulations were promulgated on August 24, 2016 by the National Privacy Commission (NPC, 2017).

Government employees play a critical role in operationalizing the Data Privacy Act, as they routinely handle sensitive and confidential information in the delivery of public services. Their level of awareness and extent of implementation of data privacy regulations are central to ensuring legal compliance and preventing unauthorized disclosure, misuse, or breaches of personal data. However, empirical evidence suggests that awareness does not necessarily translate into consistent compliance behavior. Although many government employees are aware of the existence of the DPA, gaps remain in their understanding of its specific provisions and procedural requirements (Cruz et al., 2020). Documented instances of non-compliant practices, including inappropriate sharing of confidential information through social media platforms, further highlight the discrepancy between knowledge and implementation (Barlaan, 2023). Moreover, institutional constraints such as limited training, budgetary limitations, and time pressures continue to impede effective compliance with data protection policies (Ching, Fabito, & Celis, 2018; Magnaye, 2022).

Despite growing research on data privacy compliance, relatively few studies have situated the awareness–implementation gap within a coherent theoretical framework. To address this limitation, the present study is anchored on the Comprehensive Theory of Privacy developed by James Moor (1997), particularly the Restricted Access/Limited Control (RALC) framework. Moor conceptualizes privacy not

This article is licensed under a Creative Commons Attribution 4.0 International License.

International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com
Original Article

merely as secrecy but as protection from intrusion, interference, and unauthorized access to personal information within specific contexts. In the digital environment, personal data become "greased data"—information that, once electronically captured, can easily move across systems and be repurposed beyond its original intent. This fluidity increases vulnerability and reinforces the ethical responsibility of institutions and individuals entrusted with data governance.

Central to Moor's framework is the proposition that privacy is secured through restricted access and justified through limited control. Privacy depends on clearly delineated zones that regulate who may access personal information and under what conditions. The publicity principle further asserts that rules governing private situations must be transparent and known to the individuals affected. Absent such awareness, meaningful privacy protection cannot be sustained. Within the context of this study, awareness of the Data Privacy Act reflects employees' cognitive recognition and understanding of privacy obligations and restricted access principles. Implementation, by contrast, represents the institutionalization of control mechanisms—policies, procedures, and enforcement practices—that operationalize privacy protection within local government units.

Moor also emphasizes that individuals function as moral agents within institutional environments. Employees responsible for managing citizens' personal data are not merely passive implementers of policy; rather, they are ethical actors whose decisions are shaped by organizational culture and contextual norms. Because privacy practices are inherently context-dependent, institutional environments may either reinforce or weaken compliance behaviors. Demographic characteristics such as educational attainment and employment status may influence how employees interpret regulatory requirements and internalize privacy principles. Variations in training exposure, professional experience, and organizational roles may therefore shape both levels of awareness and extent of implementation.

Guided by the RALC framework, this study assumes that awareness constitutes a foundational condition for effective implementation of the Data Privacy Act. A higher degree of awareness regarding privacy principles, restricted access zones, and regulatory obligations is expected to be associated with stronger implementation practices. By framing privacy as both a moral and institutional construct, Moor's theory provides a rigorous lens for examining not only the level of awareness among Local Government Unit (LGU) employees but also the relationship between awareness and implementation within the workplace context.

Although prior assessments have examined compliance with Republic Act No. 10173 among national government agencies, findings indicate that some institutions remain only partially compliant due to limited awareness, resource constraints, and a cautious enforcement climate (Pitogo, 2019). Comparatively fewer empirical investigations have focused on local government units, where operational structures and administrative dynamics may differ substantially. A systematic examination of awareness and implementation within LGUs is therefore essential for strengthening privacy governance at the local level.

This study addresses this gap by empirically examining the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees. Specifically, it investigates whether variations in awareness and implementation exist when employees are grouped according to sex, educational attainment, and employment status. Furthermore, it examines the relationship between awareness and implementation, consistent with the theoretical assumption that understanding privacy principles is integral to effective compliance behavior.

Research Questions

Accordingly, this study seeks to answer the following research questions:

1. What is the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees as a whole and when classified according to:
   a. Sex
   b. Educational attainment
   c. Employment status?
2. Is there a significant difference in the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees when grouped according to sex, educational attainment, and employment status?
3. Is there a significant relationship between the level of awareness and the extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees?

Methodology

Research design

This study employed a quantitative approach to investigate the level of awareness of local government unit (LGU) employees regarding the implementation of the Data Privacy Act (DPA) of 2012. Specifically, a

This article is licensed under a Creative Commons Attribution 4.0 International License.

International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com
Original Article

descriptive-correlational research design was used to examine the relationships between awareness and implementation of the DPA. According to Copeland (2022), descriptive-correlational research identifies relationships between variables in their natural settings, describing characteristics and measuring the strength and direction of associations without manipulating variables or inferring causality. This design enabled the researchers to describe current conditions related to DPA awareness and implementation, while also examining differences and associations among employee subgroups that may influence compliance. The study operationalized awareness and implementation as key constructs based on James Moor's Restricted Access/Limited Control (RALC) framework, which emphasizes that understanding privacy principles is foundational to effective institutional compliance.

Research Participants

The study participants consisted of LGU employees from a selected municipality in the province of Iloilo. A total of 75 respondents were selected through purposive sampling based on their familiarity with government workplace procedures. The sample included both permanent and probationary employees, while those employed for less than six months were excluded to ensure participants had sufficient exposure to institutional practices. The sample was diverse in terms of sex, educational attainment, and employment status to enable subgroup analyses.

Research Instrument

Data were collected using a structured questionnaire developed by the researchers, grounded on the provisions of the Data Privacy Act of 2012 and relevant literature. The instrument measured two constructs: (1) the level of awareness of the DPA, and (2) the extent of its implementation. The questionnaire consisted of 30 items divided into these two sections. These constructs were informed by Moor's (1997) framework, which emphasizes restricted access, publicity principles, and institutional control as essential dimensions of privacy protection. To ensure validity and reliability, the instrument underwent expert review and pilot testing prior to administration.

Data Gathering Procedure

The validated questionnaire was distributed to the selected LGU employees. Ethical standards were strictly observed, including obtaining informed consent from all participants and maintaining confidentiality of responses. Participants were provided with a brief orientation on the purpose of the study and were encouraged to respond honestly. The researchers emphasized the significance of the study in promoting data privacy awareness and compliance in accordance with the ethical and institutional principles outlined by Moor (1997).

Results and Discussions

Research Question 1: What is the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees as a whole and when classified according to: Sex; Educational attainment; and Employment status?

Table 1. Level of Awareness and Extent of Implementation of the Data Privacy Act of 2012 among Local Government Unit employees

Categories	N	Awareness Mean	Description	Implementation Mean	Description
1. Sex					
Male	40	4.20	HA	4.25	FI
Female	38	4.22	HA	3.97	LI
Total	78	4.21	HA	4.11	LI
2. Educational Attainment					
SHS	4	4.47	HA	4.53	FI
Vocational	4	4.8	HA	4.58	FI
College	67	4.1	A	4.07	LI
Postgrad	3	4.21	HA	3.96	LI
Total	78	4.21	HA	4.11	LI
3. Employment Status					
Casual	30	4.29	HA	4.10	LI
Contractual	39	4.18	A	4.13	LI
Permanent	9	4.05	A	4.09	LI
Total	78	4.21	HA	4.11	LI

This article is licensed under a Creative Commons Attribution 4.0 International License.

International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com
Original Article

Table 1 presents the Level of Awareness and Extent of Implementation of the Data Privacy Act of 2012 among Local Government Unit employees as a whole and when classified according to sex, educational attainment and employment status. It indicates that both males and females are highly aware of the Data Privacy Act of 2012. On the other hand, the implementation strategies of the Data Privacy Act of 2012 are fully implemented according to males with a mean of 4.25 and largely implemented according to females with a mean of 3.97. The level of awareness between male and female pertaining to Data Privacy Act of 2012 among Local Government Unit employees indicates a high level of awareness while the DPA of 2012 is largely implemented in the municipality according to males and females. Both male and female local government unit employees possessed an awareness and knowledge regarding the implementation of the Data Privacy Act of 2012 in their locality.

When it comes to educational attainment, the senior high school (M=4.67), vocational (M=4.77) and postgraduates (M=4.21) are highly aware of the Data Privacy Act of 2012 compare to college graduates. The implementation strategies are fully implemented according to senior high school graduates with a mean of 4.53 and vocation graduates with a mean of 4.58 while largely implemented to according to college graduates (M=4.07) and postgrads (M=3.96). The level of awareness of the Data Privacy Act of 2012 among Local Government Unit employees in terms of their educational attainment indicates a high level of awareness while the implementation strategies are largely implemented.

Lastly, employees with casual or job order status possess a high level of awareness about the Data Privacy Act of 2012 with a mean of 4.29 compared to contractual and permanent employees. For its implementation, the implementation strategies of the DPA of 2012 are largely implemented to all employees regardless of their employment status. The level of awareness of the Data Privacy Act of 2012 among Local Government Unit employees in terms of their employment status display a high level of awareness while the extent of implementation is largely implemented. As a whole, the Local Government Unit employees possess a high level of awareness of the Data Privacy Act of 2012 and implementation strategies are largely implemented.

Research Question 2: Is there a significant difference in the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees when grouped according to sex, educational attainment, and employment status?

Table 2. T-test, One-way ANOVA and Pearson product-moment correlation coefficient results for Significant Differences and Relationship on the Level of Awareness and Extent of Implementation of the Data Privacy Act of 2012

Categories	Awareness Mean	Sig.	Implementation Mean	Sig.	Statistical Decision
1. Sex		T-test		T-test	
Male	4.20		4.25		Not Significant
Female	4.22	t (76)=.-110	3.97	t (76)= 1.438	
Total	4.21	p= .357	4.11	p= .534	
2. Educational Attainment		One Way ANOVA		One Way ANOVA	Not Significant
SHS	4.47		4.53		
Vocational	4.8		4.58		
College	4.1	F= .642	4.07	F= .758	
Postgrad	4.21	p= .591	3.96	p= .521	
Total	4.21		4.11		
3. Employment Status		One Way ANOVA		One Way ANOVA	Not Significant
Casual	4.29		4.10		
Contractual	4.18		4.13		
Permanent	4.05	F= .216	4.09	F= .014	
Total	4.21	p= .807	4.11	p= .986	
		Pearson r		Pearson r	Significantly Related
		r= .711		r= .711	
		p= .000		p= .000	

Table 2 reports that according to T-test for paired sample findings, there is no significant difference on the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees when classified according to sex. This suggests that both male and female employees are familiar with the DPA of 2012 and its provisions and strategies are applied within the local government unit. The level of awareness and implementation are not directly influenced by sex but could be attributed to other factors such as the employee's respective roles and duties.

According to the One Way ANOVA results, there is no significant difference on the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees when classified according to educational attainment. This implies that employees, regardless of their highest

This article is licensed under a Creative Commons Attribution 4.0 International License.

International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com
Original Article

educational attainment and qualifications have a grasp on understanding the strategies and provisions of the said law. This means that all employees have equal access to information and training about DPA of 2012 regardless of their educational attainment. On the other hand, there is also no significant difference on the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees when classified according to employment status. This points out that local government unit employees demonstrate an awareness and adherence to the principles and requirements of the law regardless of the employment status. It may also indicate that awareness and implementation of the DPA of 2012 is strongly influenced by the organizational culture and workplace policy in the local government unit rather than by employment status.

As the result of the Pearson r analysis, there is significant relationship between the level of awareness and extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees. This indicates that employees who possess a higher level of awareness of the DPA of 2012 are more likely to implement and apply its provisions and strategies within their respective roles and responsibilities in the workplace. The positive relationship highlights the crucial role of awareness on the implementation of the data privacy provisions and principles in the LGU settings.

The findings of this study indicate that Local Government Unit (LGU) employees possess a high level of awareness of the Data Privacy Act (DPA) of 2012, with implementation strategies largely applied in their workplace. As shown in Table 1, females (M = 4.22) exhibited slightly higher awareness than males (M = 4.20), although the difference was not statistically significant (Table 2, t-test, p = .357). This result aligns with Abdullah, Al-Sabbagh, and Al-Shalabi (2020), who found high awareness regarding personal data privacy among respondents, with a willingness to act to safeguard their information. These findings underscore the importance of awareness as a foundation for ethical and effective privacy practices, consistent with Moor's (1997) assertion that understanding privacy principles is necessary for operational compliance.

Regarding educational attainment, Table 1 shows that senior high school (M = 4.67) and vocational graduates (M = 4.77) reported the highest awareness, while college graduates and postgraduates scored slightly lower. Despite these differences, Table 2 indicates no significant variation based on education (ANOVA, p = .591), suggesting that awareness and implementation are shaped more by institutional norms and role-based responsibilities than by formal educational background. Similarly, no significant differences were observed for employment status (Table 2, ANOVA, p = .807), highlighting that both permanent and non-permanent employees exhibit comparable levels of awareness and implementation. These findings illustrate Moor's (1997) principle that privacy is context-dependent: employees act as moral agents within institutional structures, where adherence is guided by workplace norms rather than individual characteristics.

The study also revealed a strong positive correlation between awareness and implementation (Pearson r = .711, p = .000; Table 2). Employees with higher awareness of the DPA are significantly more likely to implement its provisions in their roles. This finding supports Moor's RALC framework, which emphasizes that awareness of restricted access, publicity principles, and ethical obligations is a prerequisite for meaningful protection of personal information. Awareness enables employees to recognize privacy zones, anticipate potential risks, and apply ethical judgment in handling sensitive data, thereby translating knowledge into practical implementation.

Research Question 3: Is there a significant relationship between the level of awareness and the extent of implementation of the Data Privacy Act of 2012 among Local Government Unit employees?

Awareness and Implementation Across Demographics

The absence of significant differences in awareness and implementation across sex, education, and employment status can be interpreted through Moor's lens. Female employees may show slightly higher awareness due to greater exposure to frontline or administrative tasks, but this reflects role-based experience rather than inherent sex differences. Similarly, employees' educational attainment does not predict compliance; privacy responsibilities are shared across the institution, reinforcing that privacy is a moral and organizational obligation, consistent with the RALC framework. Employment status likewise does not influence adherence, indicating that both permanent and temporary employees operate under the same ethical and institutional expectations regarding data privacy.

The findings empirically demonstrate the relevance of Moor's (1997) RALC framework in public sector data governance. Awareness emerges as a moral foundation that informs ethical behavior, while institutional norms and policies operationalize implementation. By linking awareness to implementation across demographic groups, this study extends the theory by highlighting the role of organizational culture and contextual moral agency in shaping compliance behaviors.

This article is licensed under a Creative Commons Attribution 4.0 International License.

International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com
Original Article

The strong positive relationship between awareness and implementation underscores the importance of continuous training, clear policy communication, and reinforcement of restricted access principles. Organizational interventions should focus on strengthening both awareness and procedural compliance, ensuring that employees understand privacy zones, regulatory requirements, and ethical obligations. By fostering a culture that integrates ethical responsibility with institutional controls, LGUs can maintain high standards of data privacy regardless of employees' demographic characteristics.

Ethical Considerations

The researchers observed ethical standards by obtaining informed consent from all participants and explaining the purpose of the study. Participation was voluntary, and respondents' identities and answers were kept confidential. All collected data were used solely for research purposes and handled in accordance with Republic Act No. 10173, or the Data Privacy Act of 2012. The researchers ensured that participants' privacy, rights, and dignity were respected throughout the study.

Conclusion

This study examined the awareness and implementation of the Data Privacy Act of 2012 (RA 10173) among Local Government Unit (LGU) employees in the Municipality of Batad, Iloilo, through the lens of James Moor's Comprehensive Theory of Privacy. The findings indicate that LGU employees demonstrate a high level of awareness of the DPA, while its implementation is largely applied across the organization. No significant differences were observed in awareness or implementation based on sex, educational attainment, or employment status, suggesting that privacy practices are primarily shaped by organizational culture, institutional policies, and shared ethical responsibility, rather than by individual demographic characteristics. These results align with Moor's perspective that privacy is fundamentally a moral and social obligation, consistently practiced across roles and contexts. A central finding is the strong positive relationship between awareness and implementation, confirming that greater knowledge of the DPA translates into higher adherence in daily operations. This supports Moor's Restricted Access/Limited Control (RALC) framework, which emphasizes that effective privacy protection relies on well-defined zones of access, contextual judgment, and individual responsibility. In an era of rapidly circulating "greased data," ethical and institutional vigilance is essential to prevent inadvertent breaches and ensure that sensitive information is handled responsibly. This study acknowledges limitations. Its focus on a single municipality may limit generalizability to other LGUs or national agencies. Additionally, the quantitative approach, while effective for measuring awareness and implementation, may not fully capture employees' ethical reasoning, attitudes, or contextual decision-making. Future research could adopt qualitative or mixed-method approaches to explore these dimensions, examine organizational and technological influences, conduct comparative or longitudinal studies, and incorporate citizens' perspectives on data privacy. In conclusion, data privacy in LGUs is both a legal requirement and a moral responsibility. Integrating ethical awareness, institutional policies, and practical implementation strategies enables LGUs to cultivate a sustainable culture of privacy, protecting citizens' personal information while ensuring compliance with the DPA. Moor's Comprehensive Theory of Privacy provides a critical lens for understanding how moral, contextual, and institutional factors shape privacy practices, emphasizing that effective data protection relies not only on rules but also on ethical awareness and organizational commitment.

Recommendations

Based on these findings, several recommendations emerge: (1) Institutionalize continuous training programs and workshops to update employees on legal requirements, privacy principles, and ethical standards. (2) Codify clear, context-specific privacy policies that integrate ethical responsibility with legal compliance. (3) Implement monitoring and evaluation mechanisms, including audits and feedback systems, to reinforce adherence and identify areas for improvement. (4) Foster a culture of ethical accountability, emphasizing that privacy is a shared moral obligation rather than a procedural task. (5) Conduct awareness campaigns highlighting risks and ethical implications of mishandling personal information, reinforcing proper privacy practices and ethical

References

Abdullah, A. A., Al-Sabbagh, N. A., & Al-Shalabi, R. M. (2020). Awareness and perceptions of Saudi citizens towards their privacy rights in the digital age. Information, 11(4), Article 175.

Ahmed, F., Hussain, A., Khan, S. N., Malik, A. H., Asim, M., Ahmad, S., & El-Affendi, M. (2024). Digital risk and financial inclusion: Balance between auxiliary innovation and protecting digital banking customers. Risks, 12(8), Article 133. https://doi.org/10.3390/risks12080133

This article is licensed under a Creative Commons Attribution 4.0 International License.

International Journal of Research on Multidisciplinary Studies
Online ISSN: 3116-4137 | Print ISSN: 3116-4145
Volume 1, Issue 9, pp. 290-296, October 2026
https://ijroms.com
Original Article

Babaylan, R. I. (2018, November 29). Envisioning Philippine education. Academia.edu. https://www.academia.edu/37881603/Envisioning_Philippine_Education

Barlaan, J. V. (2023). Exploring local government employees' awareness of Data Privacy Act: Insights and recommendations in the lenses of the Theory of Planned Behavior. Remittances Review, 8(3), 425–435. https://doi.org/10.33182/rr.v8i3.29

Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. Paper presented at the annual meeting of the American Sociological Association.

Copeland, B. (2022). What is the meaning of descriptive correlational method? De Kooktips. https://bit.ly/3IRu244

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90–101.

Cruz, R. A., Reyes, M. S., & Sia, S. M. (2020). Assessing data privacy knowledge, attitudes and practices of government employees in the Philippines. Philippine Journal of Public Administration, 64(2), 147–176.

Dizon, J. M. (2018). The Philippine Data Privacy Act: Challenges and opportunities. In 2018 International Conference on Information Management and Technology (ICIMTech) (pp. 149–154). IEEE.

Foronda, S. M., Javier, N., Vigonte, F., & Abante, M. V. (2023). Implementation of Republic Act 10173 or the Data Privacy Act of 2012 in Albay Electric Cooperative (ALECO). SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4582212

Hossain, M. M., & Kaur, K. (2021). An empirical analysis of individuals' awareness and practices of personal data protection: Evidence from Bangladesh. Data in Brief, 37, Article 107150.

Liu, J., & Cai, J. (2021). Research on the current situation of Chinese consumers' awareness of personal information protection. Frontiers in Psychology, 12, Article 755474.

Magnaye, N. (2022). Anticipatory assessment through information security awareness: Approaching of local government units in a province of Oriental Mindoro. Journal of Positive School Psychology, 6(3), 3655–3664.

Miano, L. C. (2025). Awareness on data privacy vis-à-vis data management practices at a state university in Quezon province: Input towards data-driven policy and manual for good governance. Edelweiss Applied Science and Technology, 9(1). https://doi.org/10.55214/25768484.v9i1.4130

Moor, J. H. (1997). Towards a theory of privacy in the information age. ACM SIGCAS Computers and Society, 27(3), 27–32.

National Privacy Commission. (2017). National Privacy Commission toolkit: A guide for management and data protection officers.

Ngo, Q. T., Nguyen, T. H., & Nguyen, V. T. (2020). Factors influencing internet users' personal data protection behavior: Evidence from Vietnam. Telematics and Informatics, 49, Article 101423.

Olsson, E. K. (2019). The Data Privacy Act of the Philippines: An analysis of the opportunities and challenges for data protection. International Data Privacy Law, 9(1), 1–15.

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. Informing Science: The International Journal of an Emerging Transdiscipline, 19, 277–301. http://www.informingscience.org/Publications/3573

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. ACM SIGCAS Computers and Society, 31(1), 6–11.

Tomasz, Z., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. In Proceedings of the 2007 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries (SAICSIT '07) (pp. 197–204). Association for Computing Machinery. https://doi.org/10.1145/1292491.1292514

Trepte, S., & Reinecke, L. (Eds.). (2011). Privacy online: Perspectives on privacy and self-disclosure in the social web. Springer Science+Business Media.

Tsai, Y. F., & Chiu, Y. H. (2021). An empirical analysis of Taiwanese consumers' perception of privacy and data protection. Journal of Business Research, 128, 160–169.

Vicks, M. E. (2013). An examination of internet filtering and safety policy trends and issues in South Carolina's.

This article is licensed under a Creative Commons Attribution 4.0 International License.