Reframing Substantive Privacy Compliance as Dynamic Capabilities: An Integrated Conceptual Model

Uyen Nguyen Hong and Hiep Cong Pham
RMIT University, The Business School, Australia

S3974001@student.rmit.edu.au
hiep.pham@rmit.edu.vn

Abstract: Despite the widespread introduction of privacy protection laws globally, many organizations continue to treat privacy compliance as an administrative practice focusing on compulsory policies and documentations. However, many organizations have treated privacy protection compliance as a way to enhancing organizational dynamic capabilities from effectively using technology, people and processes required to implement privacy protection. Drawing on the Technology-Organization-Environment (TOE) model, Institutional Theory, and the Dynamic Capabilities View (DCV), the paper proposes that developing Substantive Privacy Compliance (SPC) through meeting regulatory, organizational, and technological requirements enables organizations enhance their dynamic capabilities. Theoretically, it fills the gap between the institutional legitimacy view and the dynamic capabilities lens, providing a comprehensive explanation of how external pressures can develop adaptive organizational capabilities. Practically, the model emphasizes the critical role of integrating privacy governance in both strategic and operational activities in enriching the firm's resilience and sustainable competitiveness.

Keywords: Privacy compliance, Dynamic capabilities, Technology-organization-environment model, Institutional theory

1. Introduction

In the modern digital economy, personal data has emerged as a strategic asset to facilitate innovation, personalisation and value creation in divergent sectors (Birch et al., 2021). Governments worldwide, in turn, have been passing stricter privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union (*General Data Protection Regulation (GDPR)*), or California Consumer Privacy Act (CCPA) in the United States ("California Consumer Privacy Act (CCPA)", 2018), all of which have required organizations to strengthen privacy management systems. Such legal frameworks are not intended to be a simple procedures checklist, they require proven accountability, internal controls and ongoing operational correspondence. Consequently, privacy compliance has ceased to be a back-office or legal issue but it has become a fundamental organizational concern directly affecting customer confidence, digital transformation, and future competitiveness (Schäfer et al., 2023).

However, organizations still found it hard to fulfill these expectations and implementations vary across industries (Li et al., 2022). Although there are management systems and standards for examples ISO/IEC 27701 (Iso/Iec, 2019) and the NIST Privacy Framework (Standards & Technology, 2020) have developed for practical controls, analysis of these information systems and data governance documents inevitably show fracturing and lack of verified and predictive measures (Raji Abraham et al., 2019). In other words, current standards (ISO, NIST) mainly describe what is expected to be performed, however, do not quantify the actual results and ability of the system to improve over time. They fail to predict whether the company is actually prepared to adjust for changes, learn and enhance their compliance behaviours. The lack of predictive measures in existing privacy management standards highlights the need to reconceptualise privacy compliance as an organizational capabilities. In addition, evidence has indicated that the compliance effort into privacy protection is rather reactive and motivated by the fright of penalty or damaged reputation instead of being strategic (von Davier et al., 2023). This type of privacy compliance could meet expectations from the external auditors but fail to facilitate substantive compliance in which privacy protection becomes an internalised ability (Klymenko et al., 2023). Consequently, organizations that are not well-prepared for preemptive privacy compliance will exhibit a corrosion of customer and partner confidence (Martin et al., 2017). More than that, such organizations are susceptible during a constant rate of technological transformation and a revolution in the regulatory demands (Saeed et al., 2023).

Information security research has long stressed technical security to enforcing privacy controls, which is mainly concerned with encryption, access control, intrusion detection and secure architecture (Delso-Vicente et al., 2025). These approaches are necessary, but they can be criticized as simply being unaware of the social, managerial and organizational processes involved in long-lasting privacy management. Moreover, many theories and frameworks have been used to explain compliance at an individual behavioural level but fail to explain compliance as an organizational process (Herath & Rao, 2009).

On the other hand, organizational compliance and legal literature focuses on the interpretation of regulations, audit processes and procedures, and relatively little on how organizations operationalize compliance (Khan, 2025). As such, privacy compliance is often predicated as a fixed requirement as opposed to an adaptive organizational capability. Such difference in technical and managerial frames causes a critical theoretical ambiguity: why some companies can maintain privacy performance whereas others fail to do so, despite comparable regulatory pressure and technological drivers. That is, the existing behaviour and technical frames fail to explain how company adapts to the regulation of privacy. In other words, there is an interdisciplinary gap, with no unified model that connects the technological, legal and managerial dimensions of privacy compliance.

This paper suggests an alternative approach to theorizing privacy compliance that views it as a dynamic capabilities within an organization rather than a requirement or status quo (Bernardo et al., 2024). In this perspective, privacy compliance entails the intuiting and continually reshaping routines to provide effectiveness in the long run (Alrub & Sánchez-Cañizares, 2025; Waldman, 2021). This interpretation keeps the legal privacy compliance with the strategic management theory as a bridge between the information security, governance and organizational capabilities building. It also gives a reason why organizations that manage privacy in a strategic manner are likely to be more successful in terms of trust, resiliency, and data-driven innovation. In general, we posit that privacy compliance is to be theorised as an organizational dynamic capabilities.

2. Background

Over the past decades, early research on privacy focused on individuals, mainly investigating to understand users' feelings and responses to privacy protection including who they trust, and under what circumstances they distribute information online (Bélanger & Crossler, 2011). Diverse theories including the Theory of Planned Behavior (Ajzen, 1991), Protection Motivation Theory (Rogers, 1983), Neutralization Theory (Altamimi et al., 2018), Control/Restricted Theory, Cognitive Theory of Multimedia (Lee et al., 2013), Deterrence Theory (Kuo et al., 2017), and Theory of Reasoned Action (Sher et al., 2017), are leveraged to comprehend how privacy concerns are perceived by individuals. While useful in explaining attitudes and intentions, these models keep privacy at the individual level and focus on user behavior. Few research has examined privacy issues at the organization level (Martin et al., 2017) and organzsational level processes underlying sustained compliance remain underexplored.

This focus begins to shift as the concept of data protection has become a strategic asset and organizations increasingly recognize that implementing privacy controls cannot be a single project (Bennett, 2018). The firms' privacy compliance involves cross-functional structures, governance routines, resource allocation as well as strategic alignment which are beyond individuals' behavioral perspectives. The classical behavioral models do not provide a description of an organization's learning and adaptation process to changes in the market, technology, and legal environment (Raju Abraham et al., 2019).

Moreover, existing research shows that firms often approach privacy safeguards as reactive and protective mechanisms focused on risk avoidance and legal defence, rather than as strategic capabilities integrated into organizational learning and innovation (Parks et al., 2017). This reactive orientation is perpetuated by regulatory environments that emphasise penalty avoidance and bureaucratic formality, including extensive documentation and audit submission requirements (Grant & Crowther, 2016). As a result, privacy management currently is seen as an administrative burden.

In spite of this, there is another perspective, companies may view privacy compliance as Substantive Privacy Compliance (SPC), not limited to procedural privacy compliance and can internalize privacy values. In other words, they are able to integrate them into its regularly repeated processes, and make compliance an adaptive capabilities. Although it has been used to explain a proactive action in sustainability, it has not been expanded in privacy research (Hyatt & Berente, 2017). Our study redefines the concept of privacy compliance in terms of a capacity building where organizations can use resources and other capabilities to improve not only compliance performance but also long-term competitiveness.

3. Proposed Substantive Privacy Model

This paper puts forward an integrated conceptual model that explains how Technology – Organization – Environment (TOE) factors (Tornatzky et al., 1990) coupled with institutional pressures ((DiMaggio & Powell, 1983) constitute the development of the SPC and how SPC, in turn, generates the emergent dynamic capabilities in organizations. The model represents an evolutionary view where privacy compliance is regarded as not an end goal but a phase in the continual process of development of adaptive capabilities.

3.1 Substantive Privacy Compliance

The conceptualisation of privacy compliance has traditionally been seen as a legal or procedural construct (Ataei et al., 2018). The current research, however, show that organizations differ in compliance adherence and internalisation (Issaoui et al., 2023). This difference leads to the concept of SPC, which is the form of compliance that goes beyond the statutory compliance and is the actual expression of privacy ideals that are reflected in the strategy of an organization, its activities, and culture (Failla, 2020).

Formal or symbolic compliance means an organizational effort to present compliance by the means of documentation, audit, or certification and not necessarily incorporating privacy values into routine decision making (Berrone et al., 2009). These compliances are usually inspired by the coercive forces and their purpose is not to pursue efficiency but rather legitimacy (Hyatt & Berente, 2017). Conversely, substantive compliance could be understood as a real behaviour alteration, which represents the level of privacy principles' learning, adoption, and performance in the organization (Chen et al., 2025). It is evident that companies go beyond the mandatory requirements such as deploying privacy-by-design principles, conduct training of employees, encouraging open communication, and introducing accountable governance systems (Yang & Kim, 2025). These activities help enhance responsibility, create more trust and develope competitive advantages for companies (Schäfer et al., 2023). Viewed through the DCV lens, SPC allows organizations to sense the changing regulatory and technological cues, seizing opportunities through reorganization privacy governance and resources, and turn organizational routines into privacy centric culture.

3.2 TOE Framework and Institutional Theory

The initial design of the TOE framework by Tornatzky et al. (1990) is a classic framework in the process of innovation adoption. It proposes three contextual dimensions, namely technology, organization, and environment, on which the assimilation of new technologies or the management practices rely. The technological environment entails internal and external technologies pertinent to the firm including information infrastructure, data management processes and automation mechanisms that enable the privacy compliance (Oliveira & Martins, 2011). All privacy governance facilitates the process of data discovery, consent management, and auditing, all of which are needed to ensure a regulatory compliance (Ali et al., 2025). The costs of implementation, complexity and compatibility with existing systems as well as skill deficiencies make implementation however a difficult process (Chander et al., 2021).

Organizational contexts are associated with internal properties of innovation adoption, such as support by the leaders, competence of employees, formalization of the processes, and communication of privacy policies (Salleh & Janczewski, 2016). These are the aspects that dictate the capabilities of an organization to integrate compliance processes and strengthen them within the organization and culture (Iwaya et al., 2022; Raddatz et al., 2025).

Lastly, the environmental context or the external pressures exerted by the governmental regulations, industry standards, and competition that compel organizations to change (Layode et al., 2024). The privacy compliance is highly affected by privacy laws and regulations. The compliance efforts are also driven by the stakeholder expectations like the customer, partner, investor and public expectations concerning the protection of the personal data (Gupta, 2025). Despite its usefulness as a descriptive framework to study contextual influences, the TOE framework has been criticized as being inactive by nature. It is adoption intention phase and does not give an insight into how organizations change and remain compliant in the process (Nguyen et al., 2022).

The Institutional Theory describes the impact of the external societal and regulatory expectations on the organizational privacy behaviour via coercive, normative and mimetic pressure (DiMaggio & Powell, 1983; Scott, 2017). These pressures in the proposed model are the environmental and institutional pressures that lead to the development of SPC. Coercive forces are obtained through legal penalties, normative through professional norm, and mimetic through imitation by peers. The examples of the coercive pressures are the legal regulations, such as the GDPR and CCPA, where the organizations are under a compulsion to observe the privacy requirements in order to avoid fines, reputational costs, and the legal penalties (Kakooza et al., 2025). The professional associations, certification programs and industry wide standards provide normative pressures that outline what is acceptable (Hyatt & Berente, 2017). Mimetic pressures are the pressure that occurs as a result of imitating others who were viewed as successful or effective in relation to their privacy practices (Zhang et al., 2022). They encourage firms to go beyond the merely symbolic compliance and internalize privacy norms, using SPC, which turns the external forces of legitimate conduct into dynamic capabilities. The Institutional Theory is

not intense on the processes of internalizing and sustaining compliance practices, although it sheds more light on the effects of compliance (Hu et al., 2007).

3.3 Dynamic Capabilities View

This part explains how SPC is the working mechanism that develops these three aspects of dynamic capabilities (DC), sensing, seizing, and transforming, in privacy management. In this paper, we apply the Dynamic Capabilities View (DCV) developed by Teece (2007) to explain the internal mechanism through which organizations transform contextual and instutional pressures into adaptive privacy routines. The difference between DC and other operational capabilities is that DC allows organizations to perceive new opportunities and threats arising, exploit them with the help of mobilizing resources and alter internal structures to remain competitive (Eisenhardt & Martin, 2000). In the context of privacy management, the DC indicate the ability of the firm to transform procedural compliance to the learning and adaptive approach that responds to evolving regulatory requirements, technological changes, and stakeholder expectations (Klymenko et al., 2023). This ability establishes in three dimensions including sensing, seizing and transforming which are interdependent (Zahra et al., 2006). Sensing refers to searching the technological and regulatory environment to determine the risk of privacy, consumer expectations, and new legal requirements (Konopik et al., 2022). Seizing means organizing technical, human, and managerial resources to create and put into effect the right compliance schemes, either privacy-by-design methodologies or automated consent management systems (Quayson et al., 2023). It also means building privacy training programs, developing data management processes, and implementing data protection technologies (Labadie & Legner, 2023). Turning them into routines and refining them on a regular basis is called transforming the privacy awareness to organizational routine and culture (Schilke & Helfat, 2025). As the previous discussion of SPC mentions, this paper will highlight the dynamic capabilities functionality, and through it, organizations can become dynamic learners as opposed to passive rule followers in reacting to the changing privacy regulations (Pigola & Da Costa, 2023).

3.4 Synthesis

A synthesis of TOE, Institutional Theory and the DCV as an integrated theoretical approach to SPC provides more insight into the matter (Abdurrahman et al., 2024). The TOE and Institutional perspectives are the two main perspectives that elaborate on the antecedent conditions, explaining why organizations are implementing compliance initiatives by the interaction of internal enablers and external pressures (Lee et al., 2023). Nevertheless, such structures do not give much information about the process of maintaining and extending compliance after adoption. They are supplemented by the DC which explains the processual and transformative mechanism that compliance is embedded through repeated learning (Kiss, 2025; Samsudin & Ismail, 2019).

Figure 1 describes how SPC mediates the influence of contextual factors such as technological, organizational, and environmental factors (based on the TOE framework) and the institutional pressures, such as coercive, normative, and mimetic forces (based on the Institutional Theory) represented under environmental factors, on a firm's dynamic capabilities.

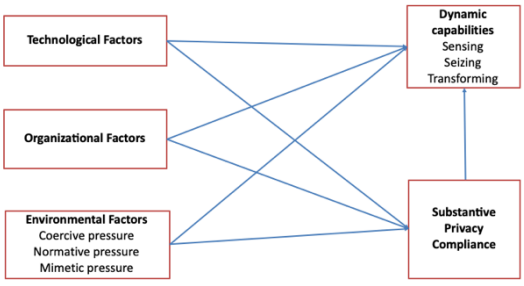

Figure 1: Proposed conceptual framework

4. Contributions

A number of implications are found in redefining the privacy compliance as DC to the theoretical advancement of privacy governance, and organizational compliance studies. First, the paper closes the divide between the privacy compliance and the DC theory, bringing the two together into a single conceptual framework. The incorporation of these areas provides this view with a stimulus to shift researchers out of the natural positions of silo thinking and interpret compliance as a dynamic organizational competency (Solaimani, 2024). Second, this stance opposes the existing perception of compliance as a reactive, punishment motivated act and suggests

a capabilities interpretation based on learning, adaptation and change. This change allows theorists to conceptualize compliance with privacy not only as the series of externally enforced norms of conduct but as a strategic resource capable of defining organizational resilience and value creation over time. Third, the DC lens offers a coping mechanism of privacy management how organizations develop, remain stable or even deteriorate with time. A DCV anticipates process of lifelong learning, which allows the richer empirical modelling and provides space to longitudinal, multilevel, process modelling research designs.

Managerially, considering privacy compliance a DC can urge executives and security leaders to reconsider the incorporation of privacy into the organization strategy and operations. Instead of handling privacy as a cost center whose main aim is to evade penalties, managers could position it as a capabilities focus which enhances customer security, facilitates digital transformation, and innovation. This view also shows how the investments should be directed at the technical controls and also to the organizational routines, cross-functional coordination and sustained training. Finally, considering privacy compliance as a dynamic capabilities gives managers the strength to develop resilience, competitive advantage based on trust, and synchronize privacy programs with the overall organizational objectives.

5. Future Directions and Conclusion

The focus on the privacy compliance as DC presents a number of potential research directions in the future. First, it is evident that there must be an effort to come up with measurement tools that can include the multidimensional character of the privacy DC. Second, empirical testing is needed to assess the way that dynamic privacy capabilities will be expressed in highly regulated industry, including fintech, health and startup companies. Third, the connection between the privacy incidents, organizational learning and capabilities enhancement is to be investigated in future research. Lastly, the advent of artificial intelligences (AI) and algorithms makes the issue of AI governance and its influence on privacy capabilities a new debate.

In conclusion, this paper suggests that privacy compliance should not be viewed as a very limited legal requirement or even a set of documented controls, but as an organizational dynamic capability, which changes regulatory requirements into organizational resilience.

Acknowledgement

The author owes a lot of credit to the direction and guidance of Dr. Minh Nhat Nguyen and Dr. Mai Thi Hoang Do, whose suggestions and positive criticism have significantly benefitted in shaping and refining this research.

Ethics declaration: This research involved human participants and received ethical approval from the RMIT, Human Research Ethics Committee. All participants provided informed consent prior to participation. The study was conducted in accordance with institutional guidelines and relevant ethical standards for research involving human subjects.

AI declaration: Artificial intelligence (AI) tools were used in a limited capacity during the development of this manuscript. Specifically, AI-assisted language tools were employed to support language refinement and clarity of expression. All conceptual development, theoretical framing, analysis, and interpretation were conducted independently by the author(s). The authors take full responsibility for the content of the manuscript.

References

Abdurrahman, A., Gustomo, A., & Prasetio, E. A. (2024). Impact of dynamic capabilities on digital transformation and innovation to improve banking performance: A TOE framework study. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(1), 100215.

Abraham, R., Schneider, C., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data Governance: A Conceptual Framework, Structured Review, and Research Agenda. *International Journal of Information Management*, *49*, 424–438.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ali, A. B. A., Ayyasamy, R. K., Akbar, R., Jebna, A. K., & Adnan, K. (2025). Cybersecurity Infrastructure Compliance Key Factors to Detect and Mitigate Malware Attacks in SMEs: A Systematic Literature Review. *SAGE Open*, *15*(1), 21582440251314671.

Alrub, Y. A., & Sánchez-Cañizares, S. M. (2025). Dynamic Capabilities and Digital Transformation: Toward Strategic Planning in the Digital Age—Evidence from Palestine. *Administrative Sciences*, *15*(1).

Altamimi, S., Storer, T., & Alzahrani, A. (2018). The role of neutralisation techniques in violating hospitals privacy policies in Saudi Arabia. 2018 4th International Conference on Information Management (ICIM),

Ataei, M., Degbelo, A., Kray, C., & Santos, V. (2018). Complying with privacy legislation: From legal text to implementation of privacy-aware location-based services. *ISPRS international journal of geo-information*, *7*(11), 442.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*, 1017–1041.

Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity*, *23*(2), 239–246.

Bernardo, B. M. V., São Mamede, H., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management—Innovation and breakthroughs across different fields. *Journal of Innovation & Knowledge*, *9*(4), 100598.

Berrone, P., Gelabert, L., & Fosfuri, A. (2009). The impact of symbolic and substantive actions on environmental legitimacy.

Birch, K., Cochrane, D. T., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society*, *8*(1), 20539517211017308.

California Consumer Privacy Act (CCPA), State of California (2018).

Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving privacy: costs of compliance and enforcement of data protection regulation. *Policy Research Working Paper*, *9594*.

Chen, J., Wang, F., Pang, S., Chen, M., Xi, M., Zhao, T., & Yin, J. (2025). A Privacy Policy Text Compliance Reasoning Framework with Large Language Models for Healthcare Services. *Tsinghua Science and Technology*, *30*(4), 1831–1845.

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, *11*(1), 28.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic Capabilities: What Are They? *Strategic Management Journal*, *21*(10-11), 1105–1121.

Failla, R. J. (2020). *The influence of organizational culture on cybersecurity governance in breached organizations*. Capitol Technology University.

General Data Protection Regulation (GDPR). European Union. https://gdpr-info.eu/

Grant, H., & Crowther, H. (2016). How Effective Are Fines in Enforcing Privacy? In *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (pp. 287–305). Springer.

Gupta, I. (2025). Data Protection and Competing Interests. In *Expectations vs Realities of Information Privacy and Data Protection Measures: A Machine-Generated Literature Overview* (pp. 65–116). Springer.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems*, *18*(2), 106–125.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153–172.

Hyatt, D. G., & Berente, N. (2017). Substantive or symbolic environmental strategies? Effects of external and internal normative stakeholder pressures. *Business Strategy and the Environment*, *26*(8), 1212–1234.

Iso/Iec. (2019). ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. In. Geneva: International Organization for Standardization.

Issaoui, A., Örtensjö, J., & Islam, M. S. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. *Future Business Journal*, *9*(1), 107.

Iwaya, L. H., Iwaya, G. H., Fischer-Hübner, S., & Steil, A. V. (2022). Organisational privacy culture and climate: A scoping review. *IEEE Access*, *10*, 73907–73930.

Kakooza, J., Bagire, V., Abaho, E., Munene, J., Tumwine, S., & Mwesigwa, R. (2025). Institutional pressures and risk governance: evidence from Uganda's financial institutions. *Journal of Money and Business*, *5*(1), 1–15.

Khan, M. N. I. (2025). Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices.

Kiss, E. M. (2025). Unpacking the micro-foundations of dynamic capabilities in retail banking: the roles of strategic alignment, leadership, and organisational structure. *International Journal of Organizational Analysis*.

Klymenko, O., Meisenbacher, S., & Matthes, F. (2023). Identifying practical challenges in the implementation of technical measures for data privacy compliance. *arXiv preprint arXiv:2306.15497*.

Konopik, J., Jahn, C., Schuster, T., Hoßbach, N., & Pflaum, A. (2022). Mastering the digital transformation through organizational capabilities: A conceptual framework. *Digital Business*, *2*(2), 100019.

Kuo, K.-M., Talley, P. C., Hung, M.-C., & Chen, Y.-L. (2017). A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *Journal of medical systems*, *41*(12), 198.

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44.

Layode, O., Naiho, H. N. N., Adeleke, G. S., Udeh, E. O., & Labake, T. T. (2024). Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information. *International Journal of Applied Research in Social Sciences*, *6*(6), 1193–1214.

Lee, E., Kim, J.-y., Kim, J., & Koo, C. (2023). Information privacy behaviors during the COVID-19 pandemic: focusing on the Restaurant Context. *Information Systems Frontiers*, *25*(5), 1829–1845.

Lee, H. A., Au, N., & Law, R. (2013). Presentation formats of policy statements on hotel websites and privacy concerns: a multimedia learning theory perspective. *Journal of Hospitality & Tourism Research*, *37*(4), 470–489.

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*, 106868.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of marketing*, *81*(1), 36–58.

Nguyen, T. H., Le, X. C., & Vu, T. H. L. (2022). An extended technology-organization-environment (TOE) framework for online retailing utilization in digital transformation: Empirical evidence from Vietnam. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 200.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic journal of information systems evaluation*, *14*(1), pp110-121–pp110-121.

Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, *26*(1), 37–65.

Pigola, A., & Da Costa, P. R. (2023). Dynamic capabilities in cybersecurity intelligence: A meta-synthesis to enhance protection against cyber threats. *Communications of the Association for Information Systems*, *53*(1), 1099–1135.

Quayson, M., Bai, C., Sun, L., & Sarkis, J. (2023). Building blockchain-driven dynamic capabilities for developing circular supply chain: Rethinking the role of sensing, seizing, and reconfiguring. *Business Strategy and the Environment*, *32*(7), 4821–4840.

Raddatz, P. A., Raddatz, N. I., Ogunade, K. M., & Kim, S. (2025). Dataveillance Duality: Navigating Employee Accountability and Privacy Concerns in the Digital Age. *J. Inf. Syst*, 1–19.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychology: A source book*, 153–176.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Salleh, K. A., & Janczewski, L. (2016). Technological, organizational and environmental security and privacy issues of big data: A literature review. *Procedia computer science*, *100*, 19–28.

Samsudin, Z., & Ismail, M. D. (2019). The concept of theory of dynamic capabilities in changing environment. *International journal of academic research in business and social sciences*, *9*(6), 1071–1078.

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business Horizons*, *66*(4), 493–504.

Schilke, O., & Helfat, C. E. (2025). Unlocking dynamic capabilities: Pathways for empirical research. In (Vol. 3, pp. 71–87): SAGE Publications Sage CA: Los Angeles, CA.

Scott, W. R. (2017). Institutional theory: Onward and upward. *The Sage handbook of organizational institutionalism*, *900*, 853–871.

Sher, M.-L., Talley, P. C., Yang, C.-W., & Kuo, K.-M. (2017). Compliance with electronic medical records privacy policy: An empirical investigation of hospital information technology staff. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, *54*, 0046958017711759.

Solaimani, S. (2024). From compliance to capability: On the role of data and technology in environment, social, and governance. *Sustainability*, *16*(14), 6061.

Standards, N. I. o., & Technology. (2020). *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Version 1.0)*. https://www.nist.gov/document/nist-privacy-frameworkv10pdf

Teece, D. J. (2007). Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance. *Strategic Management Journal*, *28*(13), 1319–1350.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The Processes of Technological Innovation*. Lexington Books.

Vietnam. (2025). *Law No. 91/2025/QH15 on Personal Data Protection*. Hanoi: Official Gazette (Công báo) Retrieved from https://congbao.chinhphu.vn/van-ban/150193

von Davier, T. Ş., Kollnig, K., Binns, R., Van Kleek, M., & Shadbolt, N. (2023). We are not there yet: The implications of insufficient knowledge management for organisational compliance. *arXiv preprint arXiv:2305.04061*.

Waldman, A. E. (2021). Privacy Compliance. In A. E. Waldman (Ed.), *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (pp. 99–160). Cambridge University Press. https://doi.org/DOI: 10.1017/9781108591386.005

Yang, W., & Kim, J. (2025). Symbolic or Substantial: Firms' Adaptive CSR Compliance Strategies in Developing Institutional Contexts. *European Journal of Sustainable Development*, *14*(3), 616–616.

Zahra, S. A., Sapienza, H. J., & Davidsson, P. (2006). Entrepreneurship and dynamic capabilities: A review, model and research agenda. *Journal of Management Studies*, *43*(4), 917–955.

Zhang, N., Wang, C., Karahanna, E., & Xu, Y. (2022). Peer privacy concern: Conceptualization and measurement. *MIS Quarterly*, *46*(1), 491–530.