



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Privacy Governance as a Source of Competitive Advantage

Susanna Ayensu Blankson¹, Jalia Nabadda², Oluwatosin Esther Ajewumi³

Southern Illinois University Edwardsville, USA

Jalia Nabadda, Saint Louis University, USA

Oluwatosin Esther Ajewumi, Olin Business School, Washington University in Saint Louis, USA

DOI : <https://doi.org/10.55248/gengpi.07.1026.3130>

ABSTRACT :

Today, many people have said that data privacy management can provide an edge to a business against its competitors. However, the timing of this is unknown. In fact, some studies indicate that privacy regulations might be more beneficial to the large companies than the small ones. This conceptual paper examines this issue. It adopts two popular concepts from strategy research: the resource-based view and the dynamic capabilities view.

First, the paper separates privacy governance from simple legal compliance. It then regards governance as a scale (or a scale-like object). On the bottom side, a firm just responds to the law. On the high end, a firm handles privacy maturely and flexibly.

The paper then merges four potential means of value of privacy governance: customer trust, reduction of risk, improved data quality, the ability to adapt. It evaluates each one based on VRIN (valuable, rare, inimitable, non-substitutable) criteria: is it valuable, rare, hard to copy, and is it hard to replace? Trust, lower risk, and better data quality do add value. But they are not always rare and difficult to duplicate. It is only an adaptive governance that will be difficult to imitate.

The paper also demonstrates that regulation has an impact. The more there is variation in rules, the more valuable the ability to coordinate is. Firms will then determine whether they have the resources to develop this ability. The paper concludes with a straightforward framework, three propositions to be tested, and ideas for future research.

Keywords: Data Privacy Governance, Competitive Advantage, Resource-based View, Dynamic capabilities, Data Protection Regulation, Firm Performance

INTRODUCTION

The management of personal data has become a strategic concern for companies, rather than a legal obligation. Industry surveys encourage this view, reporting that investment in privacy brings business value (Cisco, 2024; IAPP, 2024). It is now popular to think that privacy governance leads to competitive advantage. However, it is claimed much more often than it is tested, and the evidence suggests a more complex direction. Research into the GDPR has revealed that the costs of compliance are significant and these costs weigh more heavily for smaller businesses. The same studies reveal that regulation can be more likely to promote higher market concentration than improved conduct (Gal & Aviv, 2020; Johnson et al., 2023; Presidente & Frey, 2024). However, if regulation favours established, large companies, then governance will not be a source of advantage. Whether it becomes one is dependent on conditions that are rarely spelt out by the more optimistic accounts.

This is an indication of a bigger problem. By definition, those privacy practices mandated by law are used by everyone. It is unlikely that a resource that all competitors have will be sufficient to differentiate a firm. Thus, why should privacy governance be seen as creating an advantage, but not just an extra cost of doing business with data? Marketing and information systems research reveals that responsible data practices can help build trust and safeguard firm value (Martin et al., 2017; Martin & Murphy, 2017). However, this paper does not go far enough in understanding how governance can become a resource that can sustain an advantage. It has also grown up separately from strategy research.

This paper brings the two together. It poses one central question: When can data privacy governance serve as a sustainable competitive asset in the organisation's and regulatory framework? Here are two smaller questions: What are the mechanisms through which privacy governance can provide a competitive advantage? Second, how do governance maturity and regulatory design shape that value? It develops the answer to these questions by using the concepts of the resource-based view, which outlines the characteristics that a resource must possess to bring an advantage (Barney, 1991), and the dynamic capabilities view that outlines how firms maintain an advantage in changing environments (Teece et al., 1997; Teece, 2007).

The paper makes three contributions. First, it does not view privacy governance as an 'either-or' option; its view is that it is a continuum that can move from compliance to a developed and adaptive capability. Secondly, it integrates four mechanisms of value, and evaluates them in relation to the VRIN

criteria. Third, it introduces regulatory design as a boundary condition, and builds three propositions that link governance maturity, regulatory fragmentation, and firm resources to competitive outcomes.

LITERATURE REVIEW APPROACH

This paper is not a systematic review, but rather an integrative conceptual review. It is not to measure the frequency of occurrence of a topic in the literature but to find ideas in different fields and synthesize a single framework. It is therefore not subject to a formal search and screening process and does not claim to cover all studies in the field.

The review is based on four areas of work: Strategic management, information systems, marketing, and data-governance and privacy regulation. These fields were selected because they address various aspects of the question. Strategy research describes the value of a resource. Information systems and marketing research provide insight into the impact of privacy on trust, risk, and data use. Work on regulation explains how the legal environment influences the behaviour of firms.

The literature was structured around four questions. First, what exactly is privacy governance, and how is it different from compliance and data governance? Second, how can privacy governance be a value-creating enterprise? Third, are those mechanisms sustainable to gain a competitive advantage in the VRIN sense? Fourth, how does the regulatory setting change the value of that governance? These four questions set the structure for the sections that follow.

The review is based on peer-reviewed studies. The paper also relies on authoritative regulatory sources and practitioner reports where detail is required by current law or industry practice. These practitioner sources are only used for current context, and are not evidence of cause and effect.

THEORETICAL LENS

3.1 The Resource-Based View and Dynamic Capabilities

The resource-based view is about the inside of the firm to explain competitive advantage. It believes that an advantage is one derived from resources that are valuable, scarce, difficult to copy, and difficult to substitute (Wernerfelt, 1984; Barney, 1991). There are four VRIN (valuable, rare, inimitable, non-substitutable) conditions. When applied to privacy, the perspective shifts the emphasis from whether a company has a policy or a compliance programme as almost every company would have a policy or a compliance programme. It shifts the spotlight to the practices, knowledge, technologies and relationships that are used to manage privacy. A valuable resource that is common provides a parity with the competition. A resource that is also rare, difficult to copy and difficult to replace can provide a lasting advantage.

The view has limits, though. Priem and Butler (2001) have criticized for being circular and for failing to give much indication of how an advantage is accumulated or lost over time. The list of resources is fixed, and it does not capture the dynamic nature of markets where an advantage shifts. This limit is important for privacy, as the setting never stays still. All of these factors, regulation, technology, artificial intelligence, and customer expectations, are constantly evolving. The static resources provide little protection against that change.

The dynamic capabilities view aims to fill this gap. It is about a firm's ability to notice change, capitalise on the opportunities that the change presents, and adapt its resources in response to change (Teece et al., 1997; Teece, 2007). But these capabilities are not enough to make them an advantage on their own. The value of these depends on how fast the environment is moving, and can provide value with minimal return when the environment is stable (Eisenhardt & Martin, 2000; Schilke, 2014; Schilke et al., 2018). This paper reads privacy governance in two ways. It is an organisational resource, which can be assessed to VRIN conditions. At higher maturity, it is also a dynamic capability, which value is dependent on the context.

3.2 Privacy Governance and Governance Maturity

Privacy governance refers to the set of structures, flexible routines, controls, decision rights, and policies that govern how a firm collects, uses, shares, protects, keeps, and discards personal data. It is narrower than data governance, which covers the management of all data assets for quality and value (Abraham et al., 2019). It is wider than compliance, which means performing the bare minimum required by law. This distinction is central to the argument. Compliance establishes a ground-level level of legitimacy and reduces risk. Governance can become a part of the way things are done. If these two are treated as the same thing, then that difference does not exist, and a resource-based reading requires that these two be distinguished. Not everything that meets the minimum legal standard is necessarily rare and difficult to copy (Culnan & Williams, 2009; Martin & Murphy, 2017). The state of the field also slows progress here; privacy research occurs throughout a variety of disciplines, and key terms are not consistently used to define, or measure the core of privacy (Smith et al., 2011; Bélanger & Crossler, 2011).

Governance is best considered as a continuum, comprising four stages (Table 1). At the reactive stage; privacy work is done because of legal obligation and incidents as they come. The firm establishes roles, operating processes, controls, and monitoring at the operational level. At the integrated stage, privacy is integrated into the design, procurement, and analytics of products. The firm is constantly monitoring regulatory, technological and stakeholder shifts at the strategic level and capitalising on opportunities to use trusted, legal data for good while reshaping its practices accordingly. This continuum gives us the tool to tell ordinary compliance apart from a capability that sets a firm apart. Beyond this point, it is not about whether a firm has privacy governance, but where it is positioned within this spectrum.

Table 1. Stages of privacy governance maturity

Stage	What the firm does	How privacy is handled
Reactive Compliance	Meets legal duties, responds to incidents	Legal and incident driven
Operational governance	Sets roles, processes, controls, monitoring	Managed and repeatable
Integrated governance	Builds privacy into design, procurement, analytics	Embedded across functions
Strategic / adaptive capability	Senses change, seizes opportunities, reconfigures	Continuous and adaptive

MECHANISMS LINKING PRIVACY GOVERNANCE TO COMPETITIVE VALUE

The literature identifies four mechanisms through which privacy governance can generate value. From the point of view of VRIN, they have a distinct difference in strength, and only one fits the tough standard of a sustained competitive advantage.

4.1 Customer Trust

The most frequent argument is that open and responsible use of data builds customer trust, which fosters customer loyalty and improve performance (Martin et al., 2017; Martin & Murphy, 2017). There is good evidence of a trust effect. Converting it into an advantage is more difficult. Customers value privacy in varying ways, and say and do different things about it. However, openness can also detract from the personalised services that customers desire at the same time; when making privacy public, there is a risk that it may deter the very data sharing that is creates value (Awad & Krishnan, 2006; Smith et al., 2011). Trust does create value, then, but the value depends on the situation. It becomes rare only when the reputation of a company for trust has clearly climbed above the industry standard, which has its own upward trend as regulation begins to take hold.

4.2 Risk Reduction and Value Protection

The second claim treats governance as a mechanism to minimize exposure to breaches, fines, lawsuits, and a damaged reputation. Research indicates that breaches affect company value, can negatively impact competitors (Martin et al., 2017), and that the market responds more severely based on the severity of the breach (Rasoulia et al., 2021). This helps to retain value but does not differentiate a firm. Basic controls are now standard and sometimes mandatory by law and therefore valuable; they are not uncommon and they are not difficult to replicate. Other factors that affect recovery include a firm's size, profitability, and brand (Rasoulia et al., 2021). This brings us back to the issue that was first raised at the beginning. Risk reduction pays out more to large enterprises than it pays for good governance. It must be viewed as a measure of stability and parity, rather than any sustained advantages.

4.3 Data Quality and Analytics Enablement

The third claim is that governance fosters better quality, lineage, provenance, and legal re-use of data, and that improved data quality enhances analytics and artificial intelligence (Abraham et al., 2019; Cao & Iansiti, 2021). This is the case for the "valuable" condition because well-governed data is a more useful input. Rarity and difficulty of copying is another matter. It depends if the governance is integrated into the systems and processes of a firm or whether it is bought in as a standard control that any competitor can purchase as well. There is less evidence here than the enthusiasm implies. A large portion of it is as a result of practitioner surveys (Chaurasia, 2023; Precisely, 2024), and poor governance can be just as much of an impediment to value creation as good governance can be. (Cao & Iansiti, 2021). The mechanism is plausible, but peer-reviewed studies have not yet shown the effect clearly.

4.4 Adaptive Privacy Governance as a Dynamic Capability

The best argument is when government of privacy is an adaptive routine and not a static collection of policies. Accordingly, such a capability does three things, following Teece (2007). It feels the changes in regulations, technology, and expectations from customers. It embraces the opportunities afforded by changes – with privacy-by-design decisions, responsible data use, re-designed controls, and new products. And it reconfigures data systems, suppliers, retention rules, and roles as conditions move. This type of ability is difficult to replicate. It can be accumulated over time and through the transfer of knowledge, which is tacit and difficult to document, and it is difficult for an outsider to see the connection between what a company does and the result. (Dierickx & Cool, 1989). This is where it can really differentiate itself from a “compliance checklist” that any competitor can simply replicate. Despite that, it is still dependent on the context. It pays off best when regulation and technology are constantly changing and least when they are stable (Schilke, 2014; Schilke et al., 2018).

4.5 VRIN Assessment

Table 2 compares the four mechanisms with four VRIN conditions. The basis of each judgment is as follows:

All four mechanisms do well on value. Trust supports loyalty, risk reduction helps prevent losses, better data improves analytics, and an adaptive capability allows a firm to follow the change. Value is therefore not what separates them.

When they are rare, they begin to split. Trust is rare, and only when a company's reputation is notably better than the norm, which is increasing with the spread of privacy practices. Data quality is fairly rare, since not all companies manage data well. Risk reduction is not rare, however, as basic controls are now standard, and in many cases required by law. An adaptive capability is difficult to obtain, but only at high maturity levels, which very few firms attain.

The differences become more pronounced on imitability, and this is the deciding test. Trust and data quality are somewhat difficult to replicate, depending on how embedded they are in a company's own systems. Risk control can be easily copied, as these tend to be widely available, and many are commercially available. An adaptive capability is difficult to replicate since it has to be developed over time, and relies on knowledge that is distributed among teams, which is not readily accessible to an outsider.

The pattern is the same for substitutability. Risk reduction is the least effective, as insurance and legal defence provide a substitute for much of it. Trust and data quality are more difficult to replace, but can be achieved by a competitor in other ways. An adaptive capability is the most difficult to replace because there is no easy substitute for a solid firm that continues to sense and adjust.

Read across the four conditions, only adaptive privacy governance meets all of them at once. The others add value, but not in terms of rarity or imitability or substitutability. Hence, privacy policy alone is not the source of a lasting advantage: it is the mature capability that makes it work and evolve over time.

Table 2. The four mechanisms assessed against the VRIN criteria

Mechanism	Value	Rarity	Inimitability	Non-substitutability	Likely outcome
Customer trust	Yes, context-dependent	Variable	Moderate	Moderate	Possible differentiation
Risk reduction	Yes	Low	Low to moderate	Low	Stability/parity
Data quality & analytics	Yes	Moderate	Moderate	Moderate	Operational advantage
Adaptive privacy capability	Yes	High at maturity	High	High	Possible lasting advantage

REGULATORY ARCHITECTURE AS A BOUNDARY CONDITION

The regulatory environment plays a role in a company's ability to benefit from privacy governance. That setting determines the number of rules that the firm has to read, the amount of variance between them, and how frequently the rules change. A single regime reduces these requirements since a firm operates from a single, consistent basis. They are raised by a divided regime since the firm has to interpret, coordinate, and adjust to rules ranging from place to place. With the increasing fragmentation, the value of the mature governance capability increases, because it is more difficult to coordinate. Regulatory architecture is thus considered here to be a boundary condition, which affects the relationship between governance maturity and competitive advantage. A comparison of United Kingdom and United States demonstrates this.

5.1 United Kingdom

The United Kingdom has a single national regime. It is based on the UK GDPR and the Data Protection Act 2018, and has been recently updated by the Data (Use and Access) Act 2025 (Data (Use and Access) Act 2025). If having an aggressive baseline applies to all firms, it is not likely to be difficult for other firms to achieve or the norm. The governance advantage, then is to be derived from the improvements that the baseline does not provide, through faster adaptation, trusted data use, privacy-by-design, and the use of privacy in innovation and analytics. This is the dynamic-capability ground of the previous part of the text.

5.2 United States

This is not the case in the United States. The Federal government does not have a single privacy statute. Rather, state laws in various industries are being added to federal regulations for specific industries. Around the world, there are 20 states that had comprehensive privacy legislation by 2026. The majority follow Virginia's example but vary in thresholds, rights, enforcement, and California's has the strictest (IAPP, 2026). These differences increase coordination and interpretation workload for companies that do business in several jurisdictions in the United States. A mature capability can be valuable here, if it can, standardise controls where it can, and maintain flexibility in accordance with local rules. Fragmentation, though, tends to favour scale, since larger firms can spread the fixed cost of that capability more easily. This echoes the market-concentration effects found under the GDPR (Johnson et al., 2023).

5.3 Comparative Implications

The two regimes are compared in Table 3. Together, they show that the competitive value of privacy governance is not fixed. It varies according to the regulatory environment. It is higher when fragmentation makes coordination more beneficial, and at the same time generates scale effects that can benefit larger firms.

Table 3. Comparative regulatory architecture and strategic implications

Dimension	United Kingdom	United States	Strategic implication
Regulatory structure	Mostly national and comprehensive	Federal sector rules plus a state patchwork	The coordination burden differs
Fragmentation	Lower	Higher	Cross-jurisdiction ability is worth more
Standardisation	Higher	Lower	Firm-wide standards create efficiency
Source of advantage	Going beyond the baseline	Coordinating and adapting across rules	Supports the contingency argument
Scale effect	Present	Stronger for multi-state firms	Fixed costs may favour larger firms

The two regimes are also representative of the flexibility in the coordinating value of the capability as it changes with the architecture: greater fragmentation increases the coordinating value of a more advanced capability, while also adding scale effects that can be advantageous to firms with greater resources.

6. INTEGRATIVE FRAMEWORK AND PROPOSITIONS

The framework brings the argument together (Figure 1). Governance Maturity is at the centre. It influences competitive outcomes in four ways: Customer trust, Risk reduction, Data quality, and Adaptive capability. Then, there are two conditions that determine the value that a firm captures. The value of coordination and adaptation by regulatory fragmentation. The firm's capacity to develop the capacity is influenced by its firm resources. As a result, the framework foresees returns to privacy governance being contingent, rather than automatic. Three propositions follow.

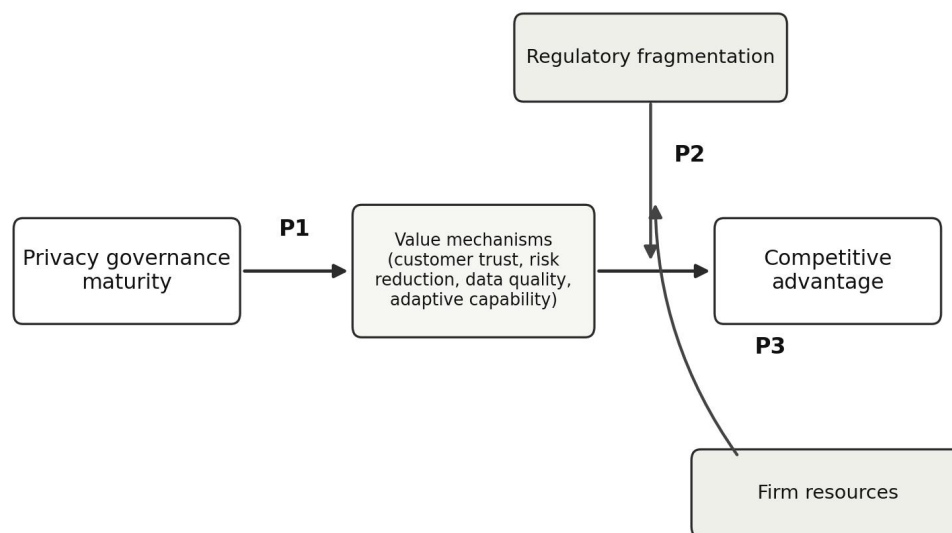
P1. The link between privacy governance and competitive advantage grows stronger as governance maturity rises. The advantage is weakest at the compliance baseline and strongest where governance works as an adaptive capability (Teece, 2007; Schilke et al., 2018).

P2. Regulatory fragmentation strengthens this link. A mature governance capability creates more value where rules are fragmented than where they are unified (Johnson et al., 2023).

P3. Firm resources strengthen the effect of fragmentation. Firms with more resources, whether financial, technological, human, or organisational, are better able to spread the fixed cost of governance and to build capability across jurisdictions. This qualifies P2, since part of the apparent advantage may reflect firm size rather than governance itself (Presidente & Frey, 2024; Johnson et al., 2023).

The framework centers on the capability of governance, while mechanisms that build that capability to create competitive outcomes are customer trust, risk reduction, data quality, and adaptive capability (Figure 1). There are coordination and adaptation benefits in a fragmented regulatory landscape, and cross-jurisdictional capability can only be achieved by firms with adequate resources to bear the fixed costs. The model, in turn, proposes three propositions and offers some insights into contingent returns to privacy governance.

Figure 1. A contingency framework for privacy governance as competitive advantage. Source: authors' own, synthesising Barney (1991), Teece (2007), Johnson et al. (2023), and Presidente & Frey (2024).



Solid arrows = direct effect (P1). Arrows that land on a path = moderating effects (P2 on the maturity-advantage link; P3 on the fragmentation effect).

7. DISCUSSION

The framework changes up the question. It takes us from "Does privacy provide value?" to "Does privacy governance provide value which cannot easily be copied by others?" The privacy investments that are made to be legitimate, to comply, or to minimise risk, do not have the characteristics of a lasting advantage. The framework proposes that there can be some real advantage only when privacy is embedded in a company's processes, data infrastructure, products, analytics, and efforts to stay in compliance with regulation.

7.1 Theoretical Implications

The framework makes three contributions to theory. For one, it sees the capability of the organisation rather than the legal responsibility as the right unit for strategic analysis. To have a policy in place is not to be an advantage to a firm, it is to have the skill that keeps the policy in place and changing. Second, it associates four mechanisms of value, which were investigated individually, together under a single heading and confronts them with a common standard. Third, it adds the regulatory setting to the resource-based view and the dynamic capabilities. It demonstrates that the worth of a capability is not set within the company. Things that work in one form of government may become important in another demanding greater coordination and adaptation.

7.2 Managerial Implications

The framework has several implications for managers. The first is a caution. Managers should not assume that having policies, certificates, or controls means that they have a strategic capability. The important question is: Is privacy embedded in decision rights, data systems, analytics, supplier management and in everyday learning? The second has to do with companies who work across fragmented rules. These companies should inquire if there are firm-wide standards that will reduce duplication but also provide for local needs. When done in this way, privacy governance is a value-adding, not a cost centre, initiative.

7.3 Policy Implications

The framework also has implications for the design of privacy policies and regulations. Fragmented and administratively complicated regimes result in high fixed costs of coordinating. The larger the firm, the more likely it is that those costs will be accommodated, and to build governance systems they can reuse. Regulators whose mission is to ensure consumer protection should therefore pay attention to the broader impact of the regulator, as this can affect entry, innovation and concentration.

8. LIMITATIONS AND FUTURE RESEARCH

This paper is conceptual. It does not examine the connection between privacy governance and firm performance, so its propositions have yet to be validated using data. The concept of maturity, centered in this, must be improved. A multidimensional measure that is developed and validated would be useful for future research in order to test the propositions properly, as a sound measure is not yet available. Another restriction is the UK/US comparison. It provides a comparison between regimes and is not a comprehensive comparative-law study, and since privacy laws evolve, the specifics of the law will become outdated.

These limits point to a clear agenda. Researchers would be able to construct and test a maturity scale, and apply it to long-term and cross-jurisdictional studies. They could examine if maturity is a factor in how well they can predict trust, data quality, innovation, and risk-adjusted performance. They could conduct mediation tests to identify whether four mechanisms mediate the effect and moderation tests to determine if the effects of fragmentation and firm resources are influencing the effect. Designs spanning multiple firms over multiple regimes would be most useful, as they would allow to disentangle the effect of capability from the effect of size.

9. CONCLUSION

This paper proposes to rethink data privacy governance as a potential strategic capability, whose value is to be measured by its maturity and the regulatory environment. Governance does not automatically result in an advantage just because it reduces risks or it shows good behaviour. It relies on how deeply privacy is into a firm's habits, and how a firm evolves its habits as technology, regulation, and expectations evolve. By joining the resource-based view with dynamic capabilities, the paper argues that mature privacy governance can become hard to imitate, while the regulatory setting decides how much that capability is worth. Seen this way, privacy governance can follow a clear path. It can begin as a compliance requirement, grow into a way of protecting value, and, at high maturity, become a source of lasting competitive advantage.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

REFERENCES

- 1) Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49(2), 424–438. <https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.07.008>
- 2) Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13–28. <https://doi.org/10.2307/25148715>
- 3) Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/https://doi.org/10.1177/014920639101700108>
- 4) 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>
- 5) Cao, R., & Iansiti, M. (2021). Data governance, interoperability and standardization: Organizational adaptation to privacy regulation. https://www.hbs.edu/ris/Publication%20Files/21-122_77bc83c9-3aec-44ad-8bec-0c0fa181c8a8.pdf
- 6) Chaurasia, J. (2023, July 12). Data governance unlocks the impact of analytics: Data strategy & insights 2023. Forrester. <https://www.forrester.com/blogs/data-governance-unlocks-the-impact-of-analytics-data-strategy-insights-2023>
- 7) Cisco. (2024, August 10). Cisco 2022 data privacy benchmark study. In Cisco. <https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html>
- 8) Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly*, 33(4), 673. <https://doi.org/10.2307/20650322>
- 9) Data (Use and Access) Act . (2025). Data (Use and Access) Act 2025. In Legislation.gov.uk. <https://www.legislation.gov.uk/ukpga/2025/18>
- 10) Dierickx, I., & Cool, K. (1989). Asset stock accumulation and sustainability of competitive advantage. *Management Science*, 35(12), 1504–1511.
- 11) Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, 21(10/11), 1105–1121. <http://www.jstor.org/stable/3094429>
- 12)
- 13) Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 16(3). <https://doi.org/10.1093/joclec/nhaa012>
- 14) GOV.UK. (2018). Data protection act 2018. In Legislation.gov.uk. GOV.UK. <https://www.legislation.gov.uk/ukpga/2018/12>
- 15) IAPP. (2024, August 10). Privacy governance report 2024 – executive summary. In Iapp.org. <https://iapp.org/resources/article/privacy-governance-report>
- 16) Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and market concentration: Intended and unintended consequences of the GDPR. *Management Science*, 69(10). <https://doi.org/10.1287/mnsc.2023.4709>
- 17) Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58. <https://doi.org/https://doi.org/10.1509/jm.15.0497>
- 18) Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/https://doi.org/10.1007/s11747-016-0495-4>
- 19) Precisely. (2024, January 4). Data quality trends for 2024. Precisely. <https://www.precisely.com/blog/data-quality/2024-data-quality-trends/>
- 20) Presidente, G., & Frey, C. B. (2022). The GDPR EFFECT: How data privacy regulation shaped firm performance globally. In CEPR. <https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally>
- 21) Priem, R. L., & Butler, J. E. (2001). Is the resource-based “view” a useful perspective for strategic management research? *Academy of Management Review*, 26(1), 22–40. <https://doi.org/10.5465/amr.2001.4011928>
- 22) Rasoulain, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2021). The effects of service crises and recovery resources on market reactions: An event study analysis on data breach announcements. *Journal of Service Research*, 26(1), 109467052110369. <https://doi.org/10.1177/10946705211036944>
- 23) Schilke, O. (2014). On the contingent value of dynamic capabilities for competitive advantage: The nonlinear moderating effect of environmental dynamism. *Strategic Management Journal*, 35(2), 179–203. <https://doi.org/10.1002/smj.2099>
- 24) Schilke, O., Hu, S., & Helfat, C. E. (2018). Quo vadis, dynamic capabilities? A content-analytic review of the current state of knowledge and recommendations for future research. *Academy of Management Annals*, 12(1), 390–439. <https://doi.org/10.5465/annals.2016.0014>
- 25) Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015. <https://doi.org/10.2307/41409970>
- 26) Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319–1350. <https://doi.org/https://doi.org/10.1002/smj.640>
- 27) Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. <https://www.jstor.org/stable/3088148>
- 28) Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, 5(2), 171–180