9-22-2023

DATA GOVERNANCE, INTEROPERABILITY AND STANDARDIZATION: ORGANIZATIONAL ADAPTATION TO PRIVACY REGULATION

Ruiqing Cao
Stockholm School of Economics, sam.cao@hhs.se

Marco Iansiti
Harvard Business School, miansiti@hbs.edu

DATA GOVERNANCE, INTEROPERABILITY AND STANDARDIZATION: ORGANIZATIONAL ADAPTATION TO PRIVACY REGULATION

Research paper

Cao, Ruiqing, Stockholm School of Economics, Stockholm, Sweden, sam.cao@hhs.se

Iansiti, Marco, Harvard Business School, Boston, USA, miansiti@hbs.edu

Abstract

The increasing availability of data can afford dynamic competitive advantages among data-intensive corporations, but governance bottlenecks hinder data-driven value creation and increase regulatory risks. We analyze the role of two technological features of data architecture that facilitate internal data governance – Application Programmatic Interfaces (APIs) that publish interdepartmental data and standardization of identity and access management (IAM) software – in shaping large data-intensive corporations' adaptation to privacy regulation. Using annual establishment data for the largest U.S. financial services corporations and the enforcement of the General Data Protection Regulation (GDPR) in 2018 as a natural experiment, we show that internal data APIs and standardization of IAM software significantly mitigate establishments' revenue loss and IT budget reduction in response to GDPR enforcement. Compliance costs measured by IT hiring increased substantially after GDPR enforcement only for firms without internal data APIs. Our findings highlight the importance of interoperability and standardization as technical conditions that facilitate dynamic integrative capability, allowing large data-intensive corporations to ensure proper data governance and adapt to privacy regulation.

Keywords: Data Governance, Privacy Regulation, Interoperability, Standardization.

1 Introduction

The pervasive presence of digital technologies increasingly disrupts traditional industries, leading to fiercer market competition and heightened consumer expectations (Vial, 2019; Kretschmer & Khashabi, 2020; Drechsler, Gregory, Wagner, & Tumbas, 2020). As a result, many legacy corporations embarked on digital transformation, aiming to use data to improve internal process efficiency, deliver higher-quality products and services, and develop innovative ML/AI solutions to automate decision-making and address customer needs (Loebbecke & Picot, 2015). At the same time, firms' aggressive exploitation of data raises ethical and societal concerns about data privacy and information security. Privacy regulations such as European Union's General Data Protection Regulation (GDPR) led to global repercussions for firms that handle personal data (Peukert, Bechtold, Batikas, & Kretschmer, 2022; Johnson, 2022). These industry and macro-level trends shape an increasingly turbulent external environment in which today's large corporations find themselves, and their ability to adapt depend on proper internal data governance.

An important bottleneck to internal data governance is the integrative capability (Helfat & Raubitschek, 2016; Helfat & Raubitschek, 2018; Vial, 2019), defined by the ability to incorporate changes to its products, resources, capabilities, and business models reliably and efficiently. Integrative capability facilitates linkages between siloed subsystems and enables intraorganizational communication and coordination. When organizations face regulatory shocks requiring stricter system-wide data governance, integrative capability can ensure efficient adaptation at a low cost (e.g., Agrawal, Gans, & Goldfarb, 2023). However, orchestrating integrative capability is not merely a strategic choice that organizations can make from the top down. Instead, it requires technological features within the enterprise architecture that may be highly inertial. To date, relatively little is understood about what technological factors contribute to integrative capability, and most studies hinting at these factors have been theoretical (Drechsler, Gregory, Wagner, & Tumbas, 2020).

We aim to fill this research gap by investigating technological features contributing to integrative capability and facilitating internal data governance. We ask two research questions: How do large data-intensive organizations adapt to privacy regulations that mandate stricter internal data governance? Which technological features can help organizations effectively adapt to privacy regulations by mitigating negative repercussions for business performance and reducing compliance costs?

To investigate these questions, we examine the empirical setting of the General Data Protection Regulation (GDPR) enforcement in 2018, which mandated stricter internal data governance requiring visibility into an organization's internal data sources and incorporation of compliance solutions with existing technologies. We propose two channels for effective organizational adaptation to privacy regulation. *First*, internal data interoperability enables organizations to meet regulatory mandates for data tracking and third-party audits. Organizations can orchestrate data interoperability using Application Programming Interfaces (APIs) to publish data across departments and functional units. *Internal data APIs* specify the technical and governance rules for organizational members to access the same underlying data without friction, automating the exchange of information across different functional units. They enable the organization to combine information across different data sources and thus gain visibility of the entire data system.

Second, standardization of identity and access management (IAM) software components ensures low-cost and efficient adaptation to privacy regulation by facilitating scalable compliance solutions that can be applied globally. When software components require updates to incorporate compliance solutions or new features to ensure compliance, standardization allows the compliance solution developed for a standardized technology component to be easily re-used by other functional units or subsystems. These technological features – internal data APIs and standardization of IAM software – contribute to integrative capability and enable organizations to adapt effectively to privacy regulation. While interoperability enables internal data tracking, standardization allows efficient global scaling of compliance solutions. Without these features, organizations may reduce value-enhancing IT

investments to lower compliance risks and compromise on revenue losses to comply with the regulation. They may also incur higher compliance costs by hiring IT workers to integrate data manually and perform regulation-related tasks.

We test these predictions by estimating the causal impact of GDPR enforcement on organizational performance and compliance costs. The enforcement of the GDPR in 2018 provides a natural experiment that allows us to identify mechanisms of organizational adaptation to a regulatory change that mandates stricter internal data governance. We use a triple differences regression framework and conduct extensive robustness checks, including matching methods such as PSM (propensity score matching) and CEM (coarsened exact matching), subsample difference-in-differences analyses, and synthetic control DID methods on aggregate corporation-level data. Our empirical sample consists of annual establishment observations from twenty-five of the largest U.S. corporations with an average founding year of 1905, which accounted for more than 36% of the total gross output of the entire U.S. finance and insurance sector. We combine establishment-level data on revenue, IT investments, and software products from Aberdeen CI Technology Database (CITDB) with three supplemental data sources: Burning Glass Technologies (BGT) data on job postings, Keystone-Microsoft survey on data architecture, and the corporations' public annual reports (10-K forms) downloaded from the U.S. Securities and Exchange Commission (SEC) website.

The final data set contains annual observations of a balanced panel of 17,311 establishments from 2016 to 2020. We identify each sample corporation's exposure to GDPR by using information from annual reports to derive the extent to which their revenues are exposed to the European market and require handling personal data. We find robust empirical evidence that the availability of APIs for publishing internal data and the standardization of identity and access management (IAM) software mitigate establishments' performance decline due to GDPR enforcement. We also find evidence that these technological features lower IT investments following GDPR enforcement. Furthermore, organizations without internal data APIs significantly increase compliance costs by hiring more IT workers, while other firms do not incur higher labor costs in response to GDPR enforcement.

Our findings provide important insights into the factors contributing to and implications of internal data governance for an organization designing a digital strategy to create and capture value from data-driven innovation. Interoperability and standardization are crucial to facilitating integrative capability within large organizations. They increase organizations' capacity to respond to system-wide regulatory shocks that require stricter internal data governance. When these technological conditions are not met, organizations may incur higher labor costs to comply with the regulation and scale back value-enhancing IT investments that risk compliance violation because they cannot orchestrate automated and error-robust mechanisms for data integration that meet regulatory requirements. Hence, our results point to these technical aspects of the enterprise data architecture as critical bottlenecks that may hinder value creation and capture from data-driven innovation such as analytics and ML technologies at the implementation stage. Our results also add to the understanding of heterogeneity in the impact of privacy regulation on large data-intensive corporations. We show that architectural and technological capabilities contributing to internal data governance can explain the variation in organizational adaptation to regulatory risks.

2 Theory Development

Digital technologies bring about disruptive changes to traditional industries and alter the competitive landscape for many large incumbent corporations. New business models increasingly emerge from the availability of data and digital technologies, replacing traditional pathways of value creation and capture (Vial, 2019; Piccoli, Rodriguez, & Grover, 2023). When customers interact with products and services through digital technologies such as IoT devices and social media (Barrett, Davidson, Prabhu, & Vargo, 2015), the process generates large amounts of data that allow firms to deliver efficient and high-quality services to customers. For legacy corporations in traditional industries, becoming "customer-centric" is one of the primary motivators for digital transformation (Kolbjornsen & Rockwood, 2019; Elm, Gaughan, & Brown, 2021). Companies that successfully develop solutions

based on large-scale user data can enhance their business performance through developing predictive analytics and AI capabilities (e.g., Wu, Hitt, & Lou, 2020; Bessen, Impink, Reichensperger, & Seamans, 2020; Gregory, Henfridsson, Kaganer, & Kyriakou, 2021; Berman & Israeli, 2022).

Data is an important source of dynamic capability that enable firms to assemble resources and leverage emergent technologies in an agile fashion in response to environmental changes (Teece, 2007; Helfat & Raubitschek, 2018; Vial, 2019). However, large legacy corporations often struggle to create value from their data assets. Their siloed and differentiated data systems are bottlenecks to delivering data as modularized digital capabilities to be shared across the organization. For these organizations, internal data governance is particularly important for ensuring the proper delivery of data as modularized resources. Data governance requires intraorganizational coordination and integrative capability, defined by "reliable, repeatable communication and coordination activity directed toward the introduction and modification of products, resources, capabilities, and business models… and encompass the capacity to establish and alter how communication and coordination activities take place" (Helfat & Raubitschek, 2018; Vial, 2019).

For large legacy corporations, internal data governance requires technical capabilities of the enterprise architecture (Mithas, Tafti, & Mitchell, 2013; Bharadwaj, El Sawy, Pavlou, & Venkatraman, 2013). Corporations have recognized the importance of a solid architectural foundation for internal data governance and ensuring data quality and representation, as the following quote by the CIO at one of the largest U.S. banks illustrates:

"You can hire a consulting company that will tell you, 'Oh, there's a big opportunity in externalizing services.' You cannot wake up one day and start externalizing stuff because you can only do it if you have a solid foundation underneath… We've invested a lot in our data quality, in our data lineage, in our data platforms, the ability to abstract the complexity of data, how we represent complex option, and how we represent trades. We decided to take a fairly modern and standardized approach to that by creating a standard which started internally." – Partner and CIO at Goldman Sachs

Technological architecture can be a critical bottleneck for large legacy corporations, especially as they move into the digital era where new digital-enabled business models reshape these organizations with increasingly decentralized infrastructural technologies and distributed data systems (Henderson & Clark, 1990; Tilson, Lyytinen, & Sørensen, 2010; Albert & Siggelkow, 2022). As large corporations embark on transformation programs (Kretschmer & Khashabi, 2020; Wessel et al., 2021), they may need to pursue both existing and new business models simultaneously to maintain business continuity. Existing firm assets can hence become barriers to transformation, when adjustment costs associated with sharing resources across both the existing and the new business model is particularly high (Eklund & Kapoor, 2019). To establish a solid architectural foundation, corporations must replace existing architectural knowledge which can be met with strong resistance and organizational inertia.

Internal APIs that publish interdepartmental data is a crucial element of the architectural foundation that can facilitate flows and linkages across disparate subsystems and data sources. These data APIs are automated interfaces that ensure low-cost and robust sharing of data across different parts of the organization, thus ensuring appropriate modularization of scalable data sources across distributed systems that increasingly characterized digitalized organizations. For example, UnitedHealth used application programmatic interfaces (APIs) to enable the re-use of the same underlying data across different applications (Optum, 2017). JP Morgan Chase used APIs to facilitate instant payment across multiple locations (J.P. Morgan, 2016). MoneyGram overhauled its IT infrastructure using APIs to streamline operational processes and improve the quality of customer experiences (Business Reporter, 2021). The following quotes from a Bloomberg news article and a technology executive at one of the largest U.S. multinational insurance corporations illustrate the importance of APIs for breaking data siloes and ensuring consistency in data sources and applications across the entire IT infrastructure at a low cost.

"Forward-thinking CIOs are freeing their data from isolated back-end systems to next-generation platforms, much like successful retail organizations… Application programming interfaces (APIs) enable many applications to consume data. It's a very modern, very powerful and ultimately a cost-

savings approach to reuse data and create consistency of data across all apps as data is externalized." – CIO of UnitedHealth Group

By June 2020, MoneyGram had already built a direct-to-consumer digital channel that provides an immersive experience that rivals those of many leading e-commerce brands. The company also proactively overhauled its supporting IT infrastructure, modernized its APIs and streamlined its operating model to support the growth of digital. – Bloomberg Business Reporter (MoneyGram)

Coordination and centralization are crucial to internal data governance, which acts in a somewhat opposite mechanism to the prevailing logic of decentralized digital organizations. The modular design principle (Sanchez & Mahoney, 1996; Baldwin & Clark, 2000; Ethiraj & Levinthal, 2004) underpins the digital organization to facilitate benefits of loosely coupled components through flexible innovation and low-cost scaling (Simon, 1962; Langlois & Robertson, 1992; Ulrich, 1995; Campagnolo & Camuffo, 2010; Zakerinia & Yang, 2023). Management of modularized organizations are often naturally decentralized as environmental changes can be addressed by confining the adaptation to localized solutions that do not involve other parts of the organization (e.g., Englmaier, Galdon-Sanchez, Gil, & Kaiser, 2019; Aghion et al., 2021). However, when the external changes are regulatory or governance-oriented, they require the entire organization to respond in a coordinated fashion.

Standardization of technology components can reduce the frictions of scaling a particular software component or sharing a data API globally across a large organization. Standardization requires centralized decisions about which technology components are used and where to source them. Once implemented, standardization lowers the costs of coordination and communication across subsystems, by lowering the structural and cognitive complexity of the enterprise architecture (Xia & Lee, 2005; Widjaja & Gregory, 2012). In the context of a dynamic environment and regulatory adaptation, the required responses are no longer sufficient at the local level, but intra-organizational spillovers of governance bottlenecks require organization-wide coordination to address (e.g., Agrawal, Gans, & Goldfarb, 2023). The following quotes from public interviews with two technology executives at Fortune 500 corporations illustrate that standardization from a centralized perspective reduces scaling frictions, and can particularly help organizations adapt to regulatory requirements by enabling the efficient scaling and re-use of compliance solutions globally.

"We've had to strike a balance between what tools are regional and what is controlled centrally. Whatever we can standardize globally reduces friction and helps us get to market even faster." – Executive VP & CIO of Prudential Financial

"One of the primary advantages of doing this from a global perspective is it gives you a considerable opportunity to leverage scale. What we generally find is that when we build a global solution, generally between 70% and 80% of that solution ends up being reusable. There are some things like regulatory requirements and privacy laws that are specific to a particular geography, but we usually have the opportunity to scale a majority of our solution with considerable speed." — Executive VP of Global Technology and Operations at Metropolitan Life Insurance Company (MetLife)

2.1 GDPR Enforcement, Data Governance, and Business Performance

Digital firms' aggressive exploitation of data raises concerns around data privacy and information security. The potential of generative innovation from the hyper-scaling of data amplifies the downside of the potential abuse of personal information. Stakeholders including policymakers and consumers have become increasingly aware of the societal risks associated with firms' collection and usage of personal data. Among the most profound regulatory changes in recent years is the General Data Protection Regulation (GDPR), introduced in 2016 and enforced in May 2018 by the European Union. Since then, different regulatory frameworks have emerged around the world, including the California Consumer Privacy Act (CCPA) and other regional laws that implement GDPR-style frameworks for protecting personal data rights.

The GDPR frames data privacy protection around mandating consumer consent for data sharing and hence putting the control of personal data in the hands of individuals themselves (Johnson, 2022). The

GDPR had profound impact on organizations not only within Europe but also global firms (which may operate outside Europe) that sell products and services to European consumers (Peukert, Bechtold, Batikas, & Kretschmer, 2022). It drastically expands the scope of privacy regulation and increased the financial penalties associated with violations relative to existing laws. The announcement of the GDPR subjects firms to substantial uncertainty around whether their current data practices are compliant with the regulation, and exposes them to compliance risks as they build new technology systems that aim at delivering customer-focused services and data-driven innovations.

The GDPR particularly affects large multinational corporations in data-intensive sectors. Large corporations are much more likely to commit to enforcement efforts than small and medium-sized enterprises (SMEs) and startups, both because they can potentially be fined a hefty amount due to their large global revenues and because they have historically installed processes and resources for adapting to regulatory changes. Relative to SMEs and startups, large corporations are also under especially intensive legitimacy scrutiny from regulators and consumers. Recent research suggests that public U.S. firms increased their attention to data privacy as a result of exposure to the GDPR (Boroomand, Leiponen, & Vasudeva, 2022). In our data, corporations with a larger share of their businesses involving European customers discuss GDPR in their annual reports (10-K forms) in greater detail since the regulation was introduced in 2016 (Appendix Figure B2). Meanwhile, the largest U.S. financial services corporations have recorded zero fines due specifically to GDPR violation up to 2020, according to a crowdsourced database on companies fined for GDPR violation.[1]

There are at least two major problems that affect large multinational corporations in complying with the GDPR. First, large corporations consist of many geographically scattered establishments, heterogeneous product lines, and diverse customer segments. They may serve customers in multiple locations, and have the same copy of personal data co-exist across jurisdictions where different privacy laws apply. The transfer of personal information from Europe to other countries is governed by the Standard Contractual Clauses (also known as the EU Model Clauses). For data to be allowed to flow across national borders for processing (Articles 44 of the GDPR), both corporations (as data controllers) and infrastructure providers (as data processers) must meet conditions of the GDPR (Articles 44). Second, under the GDPR, consumers as data subjects have the rights to obtain copies, request changes and deletion, and restrict processing and use of their personal data. To achieve this objective, firms are required to conduct data audits and be able to track data sources and the movement of all their data across different parts of the organization.

Corporations must adapt to the changing regulatory environment and uncertainty regarding externally mandated data governance standards, otherwise failing to comply with the GDPR can risk their legitimacy in the eyes of stakeholder audiences, who may withhold resources from these firms. Users may stop paying for services if they believe that the firm misused their personal data. Regulators may issue large fines if they deem the firms' data practice to be at odds with the regulation. Failure to develop compliance solutions that can be applied widely across the system can force corporations to remove parts of the system that demonstrate non-compliant data storage and processing practices, hence lowering the quality of services and customer experience. As a result, less effective data-driven capabilities and loss of digital innovation decreases consumer demand and lower revenues.

2.1.1 Effects of Application Programmatic Interfaces (APIs) and Data Interoperability

Data silos are an urgent organizational problem that plagues many legacy incumbent corporations. Distributed systems and infrastructure can lead to increasing differentiation in the enterprise architecture, causing barriers for communication and coordination around joint tasks across disparate subsystems. This problem is exacerbated by forces of digitalization that pressures traditional

[1] GDPR Enforcement Tracker: https://www.enforcementtracker.com

corporations to transition from a hierarchical and centralized form of organization into a distributed and decentralized system (Eklund & Kapoor, 2019; Giustiziero, Kretschmer, Somaya, & Wu, 2022).

Internal APIs can break down data silos by publishing data across departments, through specifying technical and governance properties that clearly define how the functionalities encapsulated within the APIs are to be shared with any organizational member with appropriate access rights. The availability of such internal data APIs facilitates integrative capability (Helfat & Raubitschek, 2018; Vial, 2019), and thus the combination of distributed resources across different parts of the organization. APIs expose data as digital capabilities, and allows users in other functional units to access these capabilities (Melville & Kohli, 2021; Benzell, Hersh, & Van Alstyne, 2022; Piccoli, Rodriguez, & Grover, 2023). Therefore, they enable multiple teams to jointly work on the same underlying data across different subsystems, without introducing technical complexities and errors that can hinder data quality.

Internal data APIs allow organizations to satisfy the GDPR mandates for internal data governance that require visibility into the entire data system for tracking information flows and conducting third-party audits. Data silos hinder regulatory compliance, because it prevents information flows across the organization and interdepartmental coordination for verifying underlying data sources used by multiple teams. APIs automate the exchange of data and information across subsystems, therefore breaking down data silos and linking data across subsystems much more efficiently than labor-intensive manual processes. On the other hand, organizations that do not have internal data APIs cannot easily comply with the GDPR, thus they may reduce investments in value-enhancing digital technologies to lower the risks of violating the regulation. Such adaptation may constrain organizational performance and lower business revenues. Therefore, we propose the following hypotheses.

Hypothesis #1a: Internal data APIs improve business performance following GDPR enforcement which imposes stricter data governance across a large corporation's entire internal data system.

Hypothesis #1b: Data-intensive large organizations without internal data APIs increase IT labor costs following GDPR enforcement to perform compliance-related tasks.

Hypothesis #1c: Data-intensive large organizations without internal data APIs reduce investments in IT assets following GDPR enforcement.

2.1.2 Effects of Standardization of Identity and Access Management (IAM) Software

In complex architectures that characterize large legacy corporations' data systems, high degrees of differentiation among existing technology components raise IT costs and introduce frictions that hinder adaptation (Xia & Lee, 2005; Widjaja & Gregory, 2012). Heterogeneity in the enterprise architecture is the result of many historical events (e.g., mergers and acquisitions) that reflected past organizational decisions but no longer fit present-day needs. These differentiated systems make it difficult for organizations and functional sub-units to set up automated processes that can respond in swiftly to changing regulatory mandates, because subsystems do not share the same technology components and communication standards.

On the other hand, standardization of technology components tame enterprise architecture complexity and lower IT costs (Boh & Yellin, 2006). Standardization facilitates technological conditions conducive to interoperability. When data and software applications use similar vendors and standardized specifications across different subsystems, it lowers the barriers to make coordinated organization-wide changes to the system and incorporating new technologies that can be easily scaled across the organization. Technology executives at large financial services corporations have recognized the importance of standardization to improve dynamic integrative capability, which allow them to introduce compliance solutions and scale them across the entire organization. For example, Morgan Stanley and Goldman Sachs manage their infrastructure by creating shared internal standards and extracting standardized assets from an integrated operator (Infrastructure Investor, 2021; High, 2023). Prudential Financial standardizes new software solutions and roll them out efficiently at a global scale (Noyes, 2021).

Standardization allows large corporations to create open architectures that facilitate the sharing of digital resources and capabilities, by reconfiguring an application into a modular asset and making it widely available to many different parts of the organization. This enables organizations to lower adaptation costs to comply with the GDPR, because they can re-use a compliance solution developed for a particular technology component (e.g., a standardized identity and access management software product) by directly applying it to other subsystems that use the same technology component. Standardization simplifies the adaptation and mitigates the challenges associated with highly differentiated subsystems that may require complex customized compliance solutions. For example, MetLife developed a global compliance solution for GDPR and rolled it out across the entire organization at low cost using a standardized approach that leverages scale (Lippert & Kane, 2017). More generally, technology components produced by a vendor with a higher industry adoption rate are more standardized, and regulatory compliance solutions for these components are easier to develop and more likely to be available through the vendor.

Organizations with low standardization may have a harder time delivering compliance solutions that cover highly differentiated subsystems and meet regulatory standards across all the customized solutions. If they cannot develop solutions that sufficiently satisfy GDPR requirements before the enforcement deadline, they may remove non-compliant IT services and products that interact with and create value from consumer data, but are at risk of violating the GDPR. As a result, GDPR enforcement can lower business revenues for these organizations. Therefore, we propose the following hypotheses.

Hypothesis #2a: Standardization of identity and access management (IAM) software improve business performance following GDPR enforcement which imposes stricter data governance across a large corporation's entire internal data system.

Hypothesis #2b: Data-intensive large organizations with low standardization of IAM software reduce investments in IT assets following GDPR enforcement.

3 Discussion and Conclusion

In this paper, we study the impact of two features of the technological architecture – internal data interoperability and software standardization – on organizational adaptation in response to system-wide regulatory shock that require stricter internal data governance. Interoperability and standardization contribute to internal data governance and thus help organizations adapt effectively to the Global Data Privacy Regulation (GDPR) enforcement. Our results show that internal data APIs and standardization of identity and access management (IAM) software significantly mitigate establishments' performance decline following GDPR enforcement. The performance decline is likely caused by lowering value-enhancing IT investments to comply with the regulation, as we find evidence that GDPR enforcement lowered IT budget among corporations with low interoperability and standardization. On the side of compliance costs, empirical evidence suggests that corporations without internal data APIs substantially increased hiring efforts in computer occupations, especially in data-intensive and regulation-related roles. Thus, corporations with low internal data interoperability incur particularly high costs to comply with the regulation.

Data governance problems in large organizations are challenging because they require joint coordination across many actors (e.g., Benfeldt, Persson, & Madsen, 2020). For legacy corporations, internal data governance is important for both regulatory compliance and digital innovation objectives, but it requires intraorganizational coordination across multiple functional units. Integrative capability (Helfat & Campo-Rembado, 2016; Helfat & Raubitschek, 2018) can create conditions that remove technological bottlenecks for data governance, but it remains somewhat neglected by the digital innovation literature that predominantly associate value creation from data and digital technologies with decentralized architecture and distributed systems. Our results show that interoperability and standardization, both requiring collective decisions beyond local units, help organizations adapt to GDPR enforcement effectively. They increase the agility with which large corporations can maintain a holistic internal view of all its data sources, and deploy compliance solutions at a global scale to meet

regulatory requirements. The qualitative data we collect from online news articles and public interviews with senior technology executives in financial services corporations align broadly with these interpretations of the quantitative results.

Data interoperability has received much attention from regulators and policymakers as a potential mandate to reign in the market power of large corporations and facilitate industry competition (e.g., Martens, Parker, Petropoulos, & Van Alstyne, 2021; Bourreau, Krämer, & Buiten, 2022). The UK Open Banking regulation specifically mandated regulatory technical standards for data interoperability in the financial services sector (Dinckol, Ozcan, & Zachariadis, 2023), but the implementation was difficult and did not lead to intended results due to large variations in incentives, architecture, and technical capabilities across industry players. Incumbent legacy firms in the established sector constitute an important context to a complex reality that can make implementing mandated regulatory standards difficult. On the other hand, standardizing technology components can lower the barriers to achieving interoperability, but it may also increase concentration in the supplier market and discourage novel solutions that depart substantially from industry standards (e.g., Miric, Ozalp, & Yilmaz, 2023), which are the opposite of regulators' objectives for fostering competition and innovation.

This paper makes several contributions. First, it provides quantitative evidence on the technological features that ensure internal data governance. While the theoretical arguments for the benefits of joint coordination and integrative capability have been put forward (Helfat & Raubitschek, 2018; Melville & Kohli, 2021; Widjaja & Gregory, 2020), there has been little empirical work measuring integrative capability or illustrating how they affect performance outcomes and adaptation costs of large corporations in response to changes in the external environment. Our results add to the understanding of technological conditions for facilitating internal data governance and responding to changing regulatory mandates.

We also contribute to the literature on the effects of privacy regulation, and the General Data Protection Regulation (GDPR) in particular. Existing research reveals the impact of GDPR on firm behavior across different contexts (Johnson, 2022; Johnson, Shriver, & Goldberg, 2023; Wang, Jiang, & Yang, 2023; Peukert, Bechtold, Batikas, & Kretschmer, 2022; Godinho de Matos & Adjerid, 2022; Burford, Shipilov, & Furr, 2022; Chen, Frey, & Presidente, 2022; Zhuo, Huffaker, & Greenstein, 2021; Koski & Valmari, 2020; Gal & Aviv, 2020; Martin, Matt, Niebel, & Blind, 2019; Jia, Jin, & Wagman, 2018). However, most of the existing literature focused on advertising and consumer-level outcomes, and identified short-run effects that indicate substantial heterogeneity in compliance efforts across markets and firms. Relatively little is known about how GDPR enforcement affected organizational strategies and performance beyond the short run among large data-intensive corporations. Our findings suggest that interoperability and standardization led to substantial difference in compliance adjustments and revenues following GDPR enforcement, and the effects persisted over time.

Our study offers a few managerial implications and practical recommendations. Digital technologies have become a source of dynamic disruption introducing new business and operating models that significantly depart from those of existing industry incumbents (e.g., Eklund & Kapoor, 2019). While incumbent corporations may embark on digital transformation to adopt new business models, these transformation programs take a very long time to implement, and may fail to yield the intended benefits. We show that integrative capability can be a useful goal of transformation, which requires joint coordination of intraorganizational actors and different functional units. Localized innovation and fragmented technology solutions are insufficient for achieving this purpose. Instead, a global approach may make it easier for organizations to achieve this goal, and facilitate digital value creation through properly orchestrating inter-system linkages and resource sharing across the organization. For example, local owners of APIs need to acknowledge that the APIs they developed will be accessed by users from other business units, and standardization requires multiple sub-units to agree upon shared design and implementation of common technology components.

Our results are also relevant to policymakers designing privacy regulations to limit societal risks of personal data exploitation. The GDPR was a pioneering regulatory framework for personal data

privacy protection, upon which more recent regulatory efforts have emerged. It is vital to understand both the intended and unintended consequences of GDPR enforcement, and technological features that can enable or hinder organizational adaptation. The incentives to standardize technology vendor choices may stifle competition in the supplier market and reduce the variety of local experimentation and data-driven innovation. We point out these potential tradeoffs that involve constraints on technology choices of large corporations to meet privacy regulation mandates. Finally, mechanisms of value creation from data and digital technologies may vary across sectors. Hence, future studies can examine how different technological features may facilitate data governance across sectors with different regulatory and market environments.

References

Agrawal, A., Gans, J. S., & Goldfarb, A. (2023). Artificial Intelligence Adoption and System-Side Change. *Journal of Economics & Management Strategy*.

Albert, D., & Siggelkow, N. (2022). Architectural Search and Innovation. *Organization Science*, *33*(1), 275–292.

Baldwin, C. Y., & Clark, K. B. (2000). *Design Rules: The Power of Modularity* (Vol. 1). MIT Press.

Barrett, M., Davidson, E., Prabhu, J., & Vargo, S. L. (2015). Service Innovation in the Digital Age: Key Contributions and Future Directions. *MIS Quarterly*, *39*(1), 135–154.

Benfeldt, O., Persson, J. S., & Madsen, S. (2020). Data Governance as a Collective Action Problem. *Information Systems Frontiers*, *22*, 299–313.

Benzell, S., Hersh, J. S., & Van Alstyne, M. W. (2022). How APIs Create Growth by Inverting the Firm. *Management Science*.

Berman, R., & Israeli, A. (2022). The Value of Descriptive Analytics: Evidence from Online Retailers. *Marketing Science*, *41*(6), 1074–1096.

Bessen, J., Impink, S. M., Reichensperger, L., & Seamans, R. (2022). The Role of Data for AI Startup Growth. *Research Policy*, *51*(5), 104513.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly*, 471–482.

Boh, W. F., & Yellin, D. (2006). Using Enterprise Architecture Standards in Managing Information Technology. *Journal of Management Information Systems*, *23*(3), 163–207.

Boroomand, F., Leiponen, A., & Vasudeva, G. (2022). Does the Market Value Attention to Data Privacy? Evidence from US-Listed Firms Under the GDPR. *Wharton Mack Institute Working Paper*.

Bourreau, M., Krämer, J., & Buiten, M. (2022). *Interoperability in Digital Markets.*

Burford, N., Shipilov, A. V., & Furr, N. R. (2022). How Ecosystem Structure Affects Firm Performance in Response to a Negative Shock to Interdependencies. *Strategic Management Journal*, *43*(1), 30–57.

Campagnolo, D., & Camuffo, A. (2010). The Concept of Modularity in Management Studies: A Literature Review. *International Journal of Management Reviews*, *12*(3), 259–283.

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *The Oxford Martin Working Paper Series on Technological and Economic Change*, *2022*(1).

Dinckol, D., Ozcan, P., & Zachariadis, M. (2023). Regulatory Standards and Consequences for Industry Architecture: The Case of UK Open Banking. *Research Policy*, *52*(6), 104760.

Drechsler, K., Gregory, R. W., Wagner, H.-T., & Tumbas, S. (2020). At the Crossroads between Digital Innovation and Digital Transformation. *Communications of the Association for Information Systems.*, *47*(1), 23.

Eklund, J., & Kapoor, R. (2019). Pursuing the New While Sustaining the Current: Incumbent Strategies and Firm Value During the Nascent Period of Industry Change. *Organization Science*, *30*(2), 383–404.

Elm, M., Gaughan, M., & Brown, T. (2021). *The Banking Heads of Digital Report*. Insider Intelligence. https://www.insiderintelligence.com/insights/bank-of-america-head-of-digital-david-tyrie-interview/

Englmaier, F., Galdon-Sanchez, J. E., Gil, R., & Kaiser, M. (2019). *Management Practices and Firm Performance During the Great Recession*.

Ethiraj, S. K., & Levinthal, D. (2004). Modularity and Innovation in Complex Systems. *Management Science*, *50*(2), 159–173.

Gal, M. S., & Aviv, O. (2020). The Competitive Effects of the GDPR. *Journal of Competition Law & Economics*, *16*(3), 349–391.

Giustiziero, G., Kretschmer, T., Somaya, D., & Wu, B. (2022). Hyperspecialization and Hyperscaling: A Resource-Based Theory of the Digital Firm. *Strategic Management Journal*.

Godinho de Matos, M., & Adjerid, I. (2022). Consumer Consent and Firm Targeting After GDPR: The Case of a Large Telecom Provider. *Management Science*, *68*(5), 3330–3378.

Gregory, R. W., Henfridsson, O., Kaganer, E., & Kyriakou, H. (2021). The Role of Artificial Intelligence and Data Network Effects for Creating User Value. *Academy of Management Review*, *46*(3), 534–551.

Gregory, R. W., Keil, M., & Muntermann, J. (2012). *Ambidextrous IS Strategy: The Dynamic Balancing Act of Developing a 'Transform & Merge' Strategy in the Banking Industry.*

Helfat, C. E., & Campo-Rembado, M. A. (2016). Integrative Capabilities, Vertical Integration, and Innovation Over Successive Technology Lifecycles. *Organization Science*, *27*(2), 249–264.

Helfat, C. E., & Raubitschek, R. S. (2018). Dynamic and Integrative Capabilities for Profiting from Innovation in Digital Platform-Based Ecosystems. *Research Policy*, *47*(8), 1391–1399.

Henderson, R. M., & Clark, K. B. (1990). Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms. *Administrative Science Quarterly*, *35*(9–30).

High, P. (2023). *Former Amazon Exec Marco Argenti Drives A Remarkable Digital Transformation At Goldman Sachs*. Forbes. https://www.forbes.com/sites/peterhigh/2023/01/25/former-amazon-exec-marco-argenti-drives-a-remarkable-digital-transformation-at-goldman-sachs/

Huang, P., Ceccagnoli, M., Forman, C., & Wu, D. J. (2022). IT Knowledge Spillovers, Absorptive Capacity, and Productivity: Evidence from Enterprise Software. *Information Systems Research*, *33*(3), 908–934.

Jia, J., Jin, G. Z., & Wagman, L. (2018). The Short-Run Effects of GDPR on Technology Venture Investment. *National Bureau of Economic Research*, *w25248*.

Johnson, G. (2022). *Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond.*

Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR. *Management Science*.

Kaganer, E., Gregory, R. W., & Sarker, S. (2023). A Process for Managing Digital Transformation: An Organizational Inertia Perspective. *Journal of the Association for Information Systems*, *24*(4), 1005–1030.

Kolbjornsen, C., & Rockwood, H. (2019). *Wells Fargo Launches New Brand Campaign, 'This is Wells Fargo,' Focused on Customer Experience*. Business Wire. https://www.businesswire.com/news/home/20190124005671/en/Wells-Fargo-Launches-New-Brand-Campaign-'This-is-Wells-Fargo'-Focused-on-Customer-Experience

Koski, H., & Valmari, N. (2020). Short-term Impacts of the GDPR on Firm Performance. *ETLA Working Papers*, *77*.

Kretschmer, T., & Khashabi, P. (2020). Digital Transformation and Organization Design: An Integrated Approach. *California Management Review*, *62*(4), 86–104.

Langlois, R. N., & Robertson, P. L. (1992). Networks and Innovation in a Modular System: Lessons from the Microcomputer and Stereo Component Industries. *Research Policy*, *21*(4), 297–313.

Lippert, M., & Kane, G. (2017). *MetLife Centers Its Strategy on Digital Transformation*. MIT Sloan Management Review. https://sloanreview.mit.edu/article/metlife-centers-its-strategy-on-digital-transformation/

Loebbecke, C., & Picot, A. (2015). Reflections on Societal and Business Model Transformation Arising from Digitization and Big Data Analytics: A Research Agenda. *The Journal of Strategic Information Systems*, *24*(3), 149–157.

Martens, B., Parker, G., Petropoulos, G., & Van Alstyne, M. W. (2021). Towards Efficient Information Sharing in Network Markets. *Working Paper*.

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers*, *21*, 1307–1324.

Melville, N. P., & Kohli, R. (2021). Models for API Value Generation. *MIS Quarterly Executive*, *20*(2).

Miric, M., Ozalp, H., & Yilmaz, E. D. (2023). Trade-Offs to Using Standardized Tools: Innovation Enablers or Creativity Constraints? *Strategic Management Journal*, *44*(4), 909–942.

Mithas, S., Tafti, A., & Mitchell, W. (2013). How a Firm's Competitive Environment and Digital Strategic Posture Influence Digital Business Strategy. *MIS Quarterly*, *37*(2), 511–536.

Morgan Stanley Infrastructure Partners: Why the Future is Digital. (2021). Infrastructure Investor. https://www.infrastructureinvestor.com/morgan-stanley-infrastructures-partners-why-the-future-is-digital/

Nagle, F. (2019). Open Source Software and Firm Productivity. *Management Science*, *65*(3), 1191–1215.

Noyes, K. (2021). *Prudential Banks on Transformation to Ensure Its Future*. The Wall Street Journal: CIO Journal. https://deloitte.wsj.com/articles/prudential-banks-on-transformation-to-ensure-its-future-01619809331?tesla=y&tesla=y

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory Spillovers and Data Governance: Evidence from the GDPR. *Marketing Science*, *41*(4), 746–768.

Piccoli, G., Rodriguez, J., & Grover, V. (2023). Digital Strategic Initiatives and Digital Resources: Construct Definition and Future Research Directions. *MIS Quarterly*, *46*(4), 2289–2316.

Sanchez, R., & Mahoney, J. T. (1996). Modularity, Flexibility, and Knowledge Management in Product and Organization Design. *Strategic Management Journal*, *17*(S2), 63–76.

Simon, H. (1962). The Architecture of Complexity. *Proceedings of the American Philosophical Society*, *106*(6), 467–482.

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

The CIO's role in digital transformation. (2017). Optum. https://www.optum.com/content/dam/optum3/optum/en/resources/articles-blog-posts/WF495098-cios-role-digital-transformation-article.pdf

The Digital Transformation: Speed and convenience drive B2C payments. (2016). J.P. Morgan. https://www.jpmorgan.com/solutions/treasury-payments/insights/digital-transformation

The evolution of MoneyGram: A digital transformation success story. (2021). Business Reporter. https://www.business-reporter.co.uk/finance/the-evolution-of-moneygram-a-digital-transformation-success-story

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research Commentary—Digital Infrastructures: The Missing IS Research Agenda. *Information Systems Research*, *21*(4), 748–759.

Ulrich, K. (1995). The Role of Product Architecture in the Manufacturing Firm. *Research Policy*, *24*(3), 419–440.

Vial, G. (2019). Understanding Digital Transformation: A Review and a Research Agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144.

Wang, P., Jiang, L., & Yang, J. (2023). The Early Impact of GDPR Compliance on Display Advertising: The Case of an Ad Publisher. *Journal of Marketing Research.*

Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Blegind-Jensen, T. (2021). Unpacking the Difference Between Digital Transformation and IT-Enabled Organizational Transformation. *Journal of the Association for Information Systems*, *22*(1), 102–129.

Widjaja, T., & Gregory, R. W. (2012). Design Principles for Heterogeneity Decisions in Enterprise Architecture Management. *33rd International Conference on Information Systems*.

Worldwide Digital Transformation Investments Forecast to Reach $1.8 Trillion in 2022, According to New IDC Spending Guide. (2022). IDC. https://www.idc.com/getdoc.jsp?containerId=prUS49114722

Wu, L., Hitt, L., & Lou, B. (2020). Data Analytics, Innovation, and Firm Productivity. *Management Science*, *66*(5), 2017–2039.

Xia, W., & Lee, G. (2005). Complexity of Information Systems Development Projects: Conceptualization and Measurement Development. *Journal of Management Information Systems*, *22*(1), 45–83.

Zakerinia, S., Yang, N., & Rao, V. R. (2023). Strategic Modular Innovation. *Working Paper*.

Zhuo, R., Huffaker, B., & Greenstein, S. (2021). The Impact of the General Data Protection Regulation on Internet Interconnection. *Telecommunications Policy*, *45*(2), 102083.