Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business

Coche, E.; Kolk, A.; Ocelík, V.

DOI
10.1057/s42214-023-00172-1

Publication date
2024

Document Version
Final published version

Published in
Journal of International Business Policy

Journal of International Business Policy (2024) 7:112–127
https://doi.org/10.1057/s42214-023-00172-1

COMMENTARY

Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business

Eugénie Coche[1] · **Ans Kolk**[1] · **Václav Ocelík**[1]

Received: 31 May 2023 / Revised: 1 August 2023 / Accepted: 11 August 2023 / Published online: 6 October 2023

Abstract
In an era of digital transformation, where data is often referred to as the 'new oil' of business, with data privacy and cybersecurity incidents recurrently making the headlines, international business (IB) scholars are increasingly grappling with the challenges posed by disparate data governance regulations. Recognizing the growing importance of this topic for IB research and policymaking, our paper seeks to offer a comprehensive examination of cross-country regulatory intricacies of data governance, frequently described by IB scholars as 'complex' and 'pluralistic' institutional contexts. This allows us to explore the various implications of diverse data governance regulations on international business, thus laying the groundwork for rigorous IB policy studies in this area. As a preliminary finding, we highlight a greater need for international cooperation, where both policymakers and multinational enterprises play a pivotal role. Using the EU data governance framework as an illustrative example, we structure our discussion around four policy areas of data governance: data use; data transfers; data storage; and data flows. We aim for this categorization to serve as a foundational basis for future IB research, aiding in tackling one of the most pressing digital challenges of this day and age: reconciling data privacy and security with data-driven innovation.

Keywords Data governance · Digitalization · Privacy · Regulation · The Brussels effect · Innovation

Introduction

Data governance, or the management, regulation, and oversight of data, is evolving into a subject of paramount importance for international business (IB). IB scholarship has identified several digitalization risks for multinational enterprises (MNEs) stemming from regulatory multiplicity, variance, and incompatibility (Luo, 2022a). Attention is also paid to the significance of disparate government regulations and policies related to data privacy and security, and of rules that limit which data may be transmitted beyond country borders and where it must be physically stored (e.g., Luo, 2022a; Nambisan, 2022; Nambisan et al., 2019). Remarkably, the critical importance of cross-country discrepancies governing data for MNEs was already acknowledged long before the advent of digital technologies, as Samiee (1984, p. 141) noted almost three decades ago that "managing international information flows in a[n] MNC is as important as managing the company's assets or its production". Since then, the value of data has risen exponentially, from being almost exclusively associated with information to being considered a key strategic asset for the creation of both private and social value (UNCTAD, 2021). Moreover, following the recognition of data as the primary ingredient of digitalization (Gestrin & Staudt, 2018), and the emergence of data-driven digital MNEs like Uber, PayPal and OpenAI, a wide array of laws has emerged that amplify the cross-border challenges observed by Samiee in 1984.

Nonetheless, existing scholarship has thus far offered a relatively limited representation of the challenges MNEs face in relation to data governance. Specifically, by largely

Accepted by Sarianna Lundan, Editor-in-Chief, 11 August 2023.
This article has been with the authors for one revision.

✉ Ans Kolk
akolk@uva.nl

Eugénie Coche
e.v.l.coche@uva.nl

Václav Ocelík
v.ocelik@uva.nl

[1] Amsterdam Business School, University of Amsterdam, Plantage Muidergracht 12, 1018 TV Amsterdam, The Netherlands

neglecting the distinct policies that govern the use, transfer, storage and flows of both personal and non-personal data, IB studies miss critical intricacies and nuances that underpin data governance. As a result, the contributions and impact of IB policy research on these topics are considerably constrained. Our goal is, thus, to enable IB scholars to inform policymakers in effectively addressing the challenges posed by data governance policies (Clegg, 2019), and more broadly, to extend current work by delving deeper into the regulatory complexity of data governance and its implications for MNEs. This paper draws on current discussions in the legal realm, where regulatory initiatives shaping data governance are high on the agenda (European Commission, 2020),[1] and directly touch upon geopolitical considerations (Ocelík & Kolk, 2023.). In doing so, we respond to calls by IB scholars for multidisciplinary perspectives, including digitalization and societal issues (Ocelík et al., 2023; Tung, 2023), and more policy-oriented research, whereby insights are provided into the forces that prompt MNEs to reconfigure their activities, strategies, and structure (Lundan & Van Assche, 2021).

While debate continues around the precise definition of 'data governance', the interpretation of this concept has evolved considerably over time. Originally, it was characterized as "the exercise of authority and control over the management of data" (DAMA International, 2009, p. 19), and primarily associated with a firm's internal management. However, recent years have seen the understanding of data governance shifting towards a holistic conceptualization: as a cross-functional framework encompassing rights, accountabilities, standards, and data policies (Abraham et al., 2019). As Zygmuntowski et al., (2021, p. 7) put it, "data governance encompasses the entirety of transnational and trans-organizational data flows, from the macro-level of nation-states to the micro-level of citizens". This evolution in definition underscores the intrinsic attributes of data governance and regulation, with various rules and standards underpinning the rights and obligations at stake in data flows.

However, while data governance encompasses regulatory frameworks pertaining to the use, management, integrity, and security of data, it is also closely intertwined with a firm's business model and risk tolerance. These interrelations were elucidated by Waldman (2021, p. 3), who observed vis-à-vis Google's data governance model that the company had "been sued for its surveillance overreach in tracking university students but only because the company's practices violated a contract, *not because they violated privacy law*" (our emphasis). Hence, regulatory compliance is one layer of data governance, which is further complemented by corporate rules, standards and practices that allow firms to collect, store and analyze data in ways that serve their business models. Importantly, the transnational nature of data governance clearly indicates high relevance for IB, and a range of possible complexities.

In the following, we will present a comprehensive overview of the cross-country regulatory intricacies at stake in this policy realm, the incentives driving these policies, and delineate their implications for MNEs and IB policy research. Given the flurry of legislation in the European Union (EU) and its extraterritorial influence (the so-called 'Brussels effect'), we use and start with the EU data governance framework to structure our subsequent discussion around four key components shaping the future of IB, namely the use, transfer, storage, and flow of data.

The 'Brussels effect'

The impact of regulatory differences on firms has been part and parcel of the IB field. The widely recognized phenomenon known as the 'race to the bottom' (Becker & Henderson, 2000; Cole, 2004) describes the tendency of MNEs to relocate to jurisdictions with lenient environmental regulations to evade compliance costs. Conversely, the more recent concept of a 'race to the top' (Bu & Wagner, 2016; Pisani et al., 2019) suggests a preference for contexts with higher standards. Location choice (of legal headquarters) has also come to the fore regarding taxation rules, especially focused on federal systems. Scholars use the term 'Delaware effect' to denote the devolution in standards within the US resulting from competition between states to relax their chartering requirements in order to attract corporations, with Delaware standing out as the most attractive location to incorporate from the perspective of management and shareholders. Conversely, the 'California effect' encapsulates the upwards ratcheting of regulatory environmental standards, with which firms choose to comply given the state's substantial market size (Bohnsack et al., 2015; Vogel, 1997). Interestingly, this incentivized firms not just to adhere to these regulations in order to retain market access, but to also subsequently lobby their home governments to adopt the same approach.

In a seminal article, Bradford (2012) extended the dynamics of the California effect by specifying the exact conditions that allow for upward regulatory convergence, coining it the 'Brussels effect'. The Brussels effect refers to the EU's unilateral power to regulate global markets, due to five critical conditions: (1) market size (the larger, the more influence); (2) regulatory capacity; (3) the

[1] We limit ourselves here to the exploration of 'core' data governance laws regarding both personal and non-personal data. Whereas numerous other laws, such as the EU AI Act deserve equal attention by IB scholars in future studies, these build upon the laws discussed here (and are more specific).

political will to create stringent standards; (4) inelastic targets, meaning that the regulated objects involve products or producers that are insensitive to regulatory changes; and (5) non-divisibility, i.e., the application of a uniform standard to govern an MNE's global conduct (Bradford, 2021). The process of such unilateral regulatory globalization unfolds in two complementary ways. A *de facto* Brussels effect occurs when MNEs are incentivized to standardize international production in accordance with a single rule. A *de jure* Brussels effect occurs when MNEs lobby their home governments to adopt EU standards so as to not be at a competitive disadvantage relative to their domestic competitors. Although it is clear that the EU's ability to unilaterally regulate international markets is not absolute, in certain policy areas, such as data protection and privacy, its influence on global regulatory standards is unparalleled.

Data privacy has become an important area of data governance in relation to 'personal data', and finds its roots in the right to privacy, protected since 1953 by Article 8 of the European Convention on Human Rights. Legislation governing an individual's right to privacy and personal data, two distinct yet interrelated rights, has evolved significantly since then, with the General Data Protection Regulation (GDPR) as the cornerstone of data privacy. In force since May 2018, the GDPR's Brussels effect resides partly in its extraterritorial application, laid down in Article 3, which reads as follows: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor *not established in the Union*, where the processing activities are related to: the offering of goods or services […] to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union" (our emphasis). MNEs processing personal data of EU citizens should comply with these obligations irrespective of the location of their headquarters. This has made the GDPR a *de facto* worldwide standard given the importance of the EU consumer market for investment and trade of countless MNEs. Moreover, it has stimulated MNEs to extend the application of GDPR rules to other markets to avoid the costs of complying with different regulatory regimes, also because many countries have adopted comparable approaches (see below).

Cross-country regulatory intricacies in data governance

The Brussels effect has come to the fore regarding four key components of data governance, i.e., data use, data transfer, data storage and data flows, which we will discuss consecutively next.

Data use

Policy developments in countries around the world demonstrate the Brussels effect. For example, Chile did not recognize data privacy as a human right until 2018, coinciding with the GDPR's entry into force (Molina, 2018). Moreover, following the GDPR's release, many countries around the globe, such as Brazil (Lei Geral de Proteçao de Dados) and Australia (Privacy Amendment Act 2017), mirrored its framework by adopting comparable legislation. At its core, the GDPR regulates how data can be used (i.e., processed) and therefore obliges firms to respect certain principles, such as to be transparent towards their users; to limit data processing to what is strictly necessary; and to ensure that data is accurate and secure (Art 5(1) GDPR). This global regulatory trend entails the aforementioned *de jure* Brussels effect. However, it should be noted that the EU's global influence in data privacy regulation already occurred with the GDPR's predecessor, the 1995 Data Protection Directive: Bradford (2012, p. 23) mentions that over 30 countries adopted similar EU-type privacy laws since its passing.

Despite growing similarities and convergence between legal systems, regulatory variance persists, with cross-border fragmentation even at stake within the EU (Custers et al., 2018). Indeed, although the GDPR is directly effective in all EU Member States and, unlike a Directive, does not need to be transposed into national law, some provisions leave room for maneuver (Boardman et al., 2020, p. 69). For example, Member States can further narrow the conditions and derogations for the lawful processing of health data, which are subject to the GDPR's most stringent rules (Art. 9(4), GDPR). On that point, there are considerable differences between the French legal system and those of the Netherlands and Luxembourg (Latham & Watkins, 2018). Similarly, the GDPR requires parental consent whenever data processing concerns a minor, but the exact definition of 'minor' varies among Member States. In the Netherlands, for instance, this applies to children under 16, while in Belgium, Denmark and Estonia, the threshold is 13 years (Milkaite & Lievens, 2019). Beyond these cross-border variations in terms of GDPR implementation, there also exist discrepancies in its enforcement, with Western European countries exhibiting stricter approaches and imposing larger fines compared to their (Central) Eastern counterparts (Daigle & Khan, 2020). The enforcement focus also seems to differ among countries, with France particularly attentive to targeted advertising, while the Netherlands primarily addresses data security breaches in public and health sectors.

Moving beyond the EU, and taking into account that at least 137 countries have data privacy legislation in place (UNCTAD, 2023), cross-border variations are magnified at the global level. Hence, for MNEs to collect and use personal data throughout regions implies the need to pay close

attention to both differences in regulatory scope (i.e., when does the law apply?) and in standards and obligations (i.e., what does the law require?). An illustrative example of the former is the EU's comprehensive notion of 'personal data' as opposed to the US' 'personally identifiable information' that precludes publicly available personal information from its scope under the California Consumer Privacy Act (CCPA) (Marini et al., 2020, p. 12). Although these definitional variations seem insignificant at first, their implications at the firm level should not be underestimated. For example, by excluding from its scope "information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public" (Art. 6-1-1303, para 17(b)), the Colorado Privacy Act seems to allow US firms to collect and use personal data from unrestricted social media profiles—i.e., open to the public—a practice that would not typically be acceptable under the GDPR (Stauss & Weber, 2022). Concerning differences in legal standards and obligations, it is worth noting that the GDPR's famous 'right to be forgotten' is absent from highly similar Argentinian or Brazilian frameworks (Daniel, 2022) and that Australia requires 'privacy impact assessments' instead of 'data protection impact' ones (Dataguidance, 2022).

In essence, legal scholars identify key differences between the value-driven EU, the market-oriented US and the authoritarian (top down) Chinese approach (Bodó et al., 2021, p. 9). In line with this, a background paper for the 2021 World Development report (Ferracane & Van der Marel, 2021) distinguishes between three different domestic data processing models: (1) an "open model, which refers to countries with no comprehensive data protection framework in place and where data protection is often treated as a consumer right (e.g., the US); (2) a conditional model, which takes a fundamental right approach to data protection and has a preventive framework in place (e.g., the EU); as well as a (3) limited model, where data protection is associated to national security and grants national governments extensive control and access rights over data (e.g., China). This accords with observations made by computer scientists regarding the 'four internets',[2] where competing views about how to govern the digital realm are championed at the national level, with significant geopolitical implications (O'Hara & Hall, 2018).

Data transfers

One way for countries to assert their sovereignty over data has been to adopt a protective stance on data transfers (i.e., cross-border data flows to a third country or an international organization), giving rise to competing and conflicting data governance regimes and types of extraterritorial influence (Arner et al., 2022). This lack of interoperability between regions gained traction with the European *Schrems I* and *II* judgments where the Court of Justice of the EU (CJEU) (2015, 2020) invalidated existing mechanisms for lawful data transfers between the EU and the US, and introduced a high threshold for transatlantic data transfers. Whereas *Schrems I* invalidated the EU-US Safe Harbor Agreement in 2015, the follow-up judgment invalidated the 2016 EU-US Privacy Shield, relied upon by more than 5300 companies, and imposed very strict standards on the use of so-called Standard Contractual Clauses, one of the few GDPR mechanisms for lawful data transfers to third countries (Chander, 2020). In brief, the CJEU requires companies transferring personal data of EU citizens to ensure that the data in question receive a level of protection that is 'essentially equivalent' to that of the EU, which required extensive clarifications by the European Data Protection Board (EDPB, 2021).

Besides creating uncertainty for firms, especially European ones, this judgment exposes the international difficulties in safeguarding data privacy and data security, with both aspects being ultimately dependent on foreign governments' national security policies that often require (extensive) data access. As Chander (2020) underlined, on trial in *Schrems II* was ultimately not Facebook but the US government, whose far-reaching surveillance laws were exposed in 2013 by Edward Snowden (Dyer, 2013). Similarly, China's 2017 National Intelligence law requires "any organisation or citizen to support, assist, and cooperate with state intelligence work according to law" (Art. 7). This broadly phrased requirement has led to Chinese-owned TikTok App being subjected to global scrutiny, stemming from concerns over potential foreign espionage. Concerns escalated after the revelation that TikTok's employees at the corporate level, including those of its parent company ByteDance in China, could access users' data collected elsewhere (Milmo, 2022). Hence, ambiguities arose as to whether the company could ultimately prevent data access by third-country governments, with law professor Michael Veale clarifying that "contracts between a Chinese and a European company can't prevent state access" (Milmo, 2022). This has prompted the EU's GDPR investigations into TikTok's data transfers (Data Protection Commission, 2021).

The relevance of data transfer policies to IB must be understood in light of what Ursula von der Leyen (2022) observed in relation to subsidiaries within an MNE, namely that data transfer rules apply where "a company in the EU allows access to personal data under its control to an affiliated company (e.g., a parent company) that is located outside the EU". Consequently, MNEs face heightened risks for data transfer breaches, especially in view of their exposure to various data transfer regimes. Ferracane and Van de

[2] The authors make a further distinction between how Silicon Valley treats personal data versus how the federal government in Washington DC does.

Marel (2021), already mentioned under data use, also classify countries' "cross-border data transfer models" as being either (1) "open", meaning that companies are somehow free to decide whether and how they transfer data to third countries (e.g., Australia, Mexico, the US); (2) "conditional", which implies ex-ante requirements that must be fulfilled prior to data transfers taking place (e.g., Argentina, the EU, Singapore, Turkey); or (3) "limited" in the sense that data transfers are either forbidden or subject to prior approval by national governments based on security assessments (e.g., Brunei, China, Russia, Tunisia). Interestingly, as illustrated by Mexico and Singapore, a country may be "limited" or "conditional" with respect to its domestic use of data (see the previous section) but "open" in terms of cross-border data transfers.

From an EU perspective, although the Commission's latest adequacy decision, allowing lawful data transfers between the EU and the US "without any further conditions or authorizations", entered into force on 11 July 2023, the *Schrems II* case has global ramifications that extend well beyond this transatlantic relationship to all "third countries that lack an adequacy decision [with the EU], thus including China, India and other major EU trading partners" (Kennedy-Mayo & Swire, 2021). Regardless of whether the discussion involves the US or China, the data transfer requirements under EU law and the resulting uncertainties, such as the announcement of an impending *Schrems III* case (NOYB, 2023), have created concerns about the EU's de facto imposition of data storage requirements, more commonly referred to as data localization measures (Chander, 2020). These will be discussed in more detail next.

Data storage

Data localization refers to the process of physically localizing data. Data localization policies mandate firms to process and store data locally, i.e., where the data originate. Different types of data localization measures exist, applying to different types of data and ranging from rather light requirements, such as the need to store a local copy of data, to very strict ones, such as a total ban on data transfers (Wu, 2021). Whereas the CJEU did not explicitly impose data localization requirements in *Schrems II*, many have argued they exist tacitly (Kennedy-Mayo & Swire, 2021). Indeed, "if there is no data transfer outside the EU, then there is no need to take the risk that the transfer will be found invalid by a data protection authority or a court" (Chander, 2020, p. 777). A particularly sensitive issue following the CJEU judgments and subsequent recommendations by the European Data Protection Board (01/2020) is the situation of cloud service providers, whereby most EU firms, as well as national (Conseil d'Etat, 2020) and EU organizations (EDPS, 2021) rely on US cloud giants to store their data, with Amazon Web Services being a prime example (Vasylyk, 2022).

Given the aforementioned uncertainties about data transfers, recent developments suggest firms are moving towards localizing data. An example is the Oracle EURA Cloud Service, which addresses customers' growing need "for cloud services that are designed for the EU, located in the EU, and operated by EU personnel" (OCI, 2023). By using this service, firms ensure that personal data of EU citizens is stored in EU datacenters and only accessible to EU-based persons. Similarly, Microsoft announced its 'EU Data Boundary solution', which took effect in January 2023 and is designed to "take advantage of the full power of the public cloud while respecting European values and sovereignty needs" (Brill & Chapple, 2022). By doing so, Microsoft aims to offer its private and public sector customers the chance to meet regulatory requirements and industry-specific standards, in addition to the 17 datacenters it has constructed in Europe (Brill & Chapple, 2022). Similarly, TikTok's 'Project Clover' is aimed at strengthening the security of EU citizens' data, while 'Project Texas' addresses US concerns (Bertram, 2023; Perault & Sacks, 2023).

The reasons for implementing data localization policies are varied and complex. They include national security concerns related to law enforcement; the need to guarantee citizens' privacy rights; and the desire to establish countries' technological sovereignty. The result, however, constitutes "a patchwork of national regulations […] that pose challenges to the free, decentralized and open spirit of the Internet, and create obstacles for a potentially beneficial flow of data across borders" (UNCTAD, 2021, p. 191). It is important to distinguish between data transfers and storage requirements, as they are closely related yet distinct concepts. China's Data Security Law provides an example of this distinction, requiring 'core' and 'important' data generated in China to be stored there, with separate rules governing data exports (Junck et al., 2021). Ferracane and Van de Marel (2021) do not distinguish between a country's data storage and data transfer policies, but rather treat the former as a subset of the latter by associating data localization requirements to closed data transfer models, which is not the case per se. Even a country with an open data transfer model, such as Australia, can impose data localization requirements on specific types of data, as is the case with health data under the Australia My Health Records Act 2012. This shows the importance of unravelling the intricacies of data governance as emphasized in our paper.

The complexity of attributing data localization policies (which can also apply to only one sector or type of data) to a single country's data governance framework, has come to the fore in a 2022 OECD trade policy paper (López González et al., 2022). It provided a 'preliminary mapping' of four types of data localization measures. If we couch them in the

terminology adopted above, the first category is 'open', in the sense that there are no local data storage requirements imposed on firms, which are instead obligated to guarantee access to data by local authorities (e.g., Mexico regarding telecommunication data). The second type is 'conditionally open', signifying that firms are by default free to transfer and store data abroad but must also maintain a local copy of certain types of data (e.g., Sweden regarding accounting data). The third category, somewhat stricter, could be described as 'conditionally closed', with similar local copy requirements as the former but combined with certain limitations on data transfers (e.g., Australia regarding health record data). The fourth type is the strictest and most limited: local data storage requirements are standard and cross-border data transfers are the exception (e.g., Indonesia). Despite such a categorization, which allows us to 'zoom out', it is crucial to bear in mind that, unlike the previous two models regarding data use and transfer, it does not allow us to "singularly identify any given country's approach to data localization"; instead, "different approaches tend to apply to different types of data, even within the same jurisdiction" (López González et al., 2022, p. 7).

As of yet, there are no formal data localization requirements at the EU level. France introduced the 'Trusted Cloud doctrine' in 2021, which mandates cloud service providers to obtain a certification label when providing services to state agencies. To receive this label, firms must localize data within the EU and not be foreign-owned by more than 39%. The EU is exploring whether to adopt similar certification schemes (Propp, 2022a), which indicates that digital sovereignty ambitions are not solely constrained to personal data, as was the case under *Schrems II*, but also to non-personal data. Indeed, French data localization requirements apply to the processing of "sensitive data, including personal data of French citizens and economic data relating to French companies" (Propp, 2022a). This broadening can also be seen in the EU Data Governance Act (DGA), which imposes GDPR-like requirements for the transfer of non-personal data (Art. 5(9–12) DGA). Despite the "chilling effect" of such mechanisms on international transfers of non-personal data, with serious consequences for IB (Heiber & Workman, 2023), a potential Brussels effect has been suggested, which "might push certain third countries to strengthen their IP [Intellectual Property] and trade secrets protections to the levels similar to those in the EU" (Vogelezang, 2022). Unlike the GDPR, which is primarily aimed at personal data protection, the DGA is primarily aimed at encouraging the flow of both personal and non-personal data for the sake of innovation.

Data flows

In February 2020, the European Commission (2020) unveiled its vision for a single European data space, with the aim of promoting the free flow of both personal and non-personal data between Member States and industrial sectors by 2030. It seeks to expedite innovation, empower citizens, promote data security, and transform the EU into a global role model for a society powered by data (European Commission, 2020). In this context, two complementary EU regulations, the Data Act (DA) and the DGA, are expected to significantly change the data governance landscape. The DA requires manufactures of Internet of Things devices to give their users access to data generated by them, whether personal or non-personal, and share these with third parties (European Commission, 2022a). Besides giving users and businesses more control over their data, such data-sharing obligations aim to unlock competitive opportunities for after-market services and encourage firms to innovate based on industrial data insights. However, this approach also poses risks for consumers, whose data privacy might be compromised, and firms, which run the risk of trade secrets being 'stolen'. This is where the DGA comes into play, to develop "the processes and structures to facilitate data-sharing by companies, individuals and the public sector" (European Commission, 2022b). To this end, it introduces 'data intermediation' actors: neutral third parties connecting individuals and companies with data users (European Commission, 2022c). The DGA furthermore advances the concept of 'data altruism' to motivate individuals and firms to share their data for the betterment of society (European Commission, 2022c).

In view of the cross-country challenges encountered by financial firms—the first sector on which customer-centric data-sharing obligations were imposed (Buckley et al., 2021)—the fact that these Acts are Regulations and not Directives is likely to be embraced by MNEs. Indeed, as illustrated through the Revised Payments Services Directive (PSD2), which requires banks to share some customer data with third parties for the sake of innovation, competition and security (Directive EU 2015/2366), Directives entail significant cross-border challenges, ranging from definitional variations (Stastny, 2022) to lack of interoperability standards. On top of these complexities at the EU level, PSD2 illustrates a crucial obstacle in data-sharing laws (also expressed in relation to the DA and the DGA), i.e., personal data protection laws, intellectual property rights (IPR), commercial confidentiality and business opportunities for innovation (Bertuzzi, 2022; Vardanyan & Kocharyan, 2022).

Despite the practical challenges in implementation, data-sharing initiatives, particularly in the financial sector, have been adopted in various locations, such as Brazil, Canada, Japan, Hong Kong, and the UK (Buckley et al., 2021), with each having a unique approach in terms of scope and obligations. Over 60 countries worldwide are currently implementing open banking initiatives (Ohab & Shariff, 2023). In this regard, three models can be distinguished (EPA Asia,

2021, pp. 7–10). First, a prescriptive model found in the EU, the UK, and Australia, based on regulations that require financial institutions to share permitted consumer data with authorized third parties. It is characterized by some degree of interoperability standardization. Notably, Australia extends the data-sharing mandates beyond finance through a consumer data right framework (Buckley et al., 2021). Second, a facilitative model, present in Singapore, Hong Kong, and Japan, encourages the sharing of data through industry-wide government guidance and recommendations without imposing any obligations on firms to do so. Finally, a market-driven approach to data-sharing exists when the government adopts a 'wait and see' stance, leaving it up to market players to decide whether or not to share their data with others. This data-sharing model, present in the US and China, is primarily shaped by industry players and is characterized by a high degree of fragmentation in terms of interoperability standards (Buckley et al., 2021). Based on experiences from other jurisdictions, Canada is currently shaping its data-sharing model through a hybrid regulatory–industry driven approach, which incorporates both European and US components (Ohab & Shariff, 2023).

Implications for MNEs, IB, and policy

Digitalization has emerged as a pivotal topic in the IB literature and one might therefore expect that, alongside research exploring its impact on internalization (Hennart, 2019; Monaghan et al., 2020; Tatarinov et al., 2022), corporate taxation (McGaughey & Raimondos, 2019), and entry modes (Brouthers et al., 2022), data governance would also be of much interest. However, the scant attention paid to the intricate regulatory challenges at play contrasts sharply with IB's long-standing focus on IPR and on the dynamics between IPR strategies and IPR regimes (Cui et al., 2022). Scholars in the field do occasionally refer to disparate data governance laws at the macro level, such as India's Personal Data Protection Bill, China's state-led approach to data-sharing, US digital privacy laws and the EU's GDPR (Cha et al., 2023; Nambisan & Luo, 2021); the differences in regulatory environments between developed and developing countries (Cumming et al., 2023); or the importance of national institutions concerning IB in the digital age (Meyer et al., 2023). Calls are also made to study data localization, antitrust, data security and privacy issues, as these are becoming increasingly important in the context of cross-border e-commerce activities (Cumming et al., 2023).

Regarding IB implications, some scholars highlight compliance issues (George & Schillebeeckx, 2022; Luo, 2022a), including security, reputational and legal costs in case of infringements (Madan et al., 2022), while others point out the effects on MNEs' internationalization strategies (Wu & Gereffi, 2018) and global value chain activities (Luo, 2022a). An increase in deglobalization has also been mentioned, as disparate data privacy regulations lead to MNEs and their partners being subject to conflicting market pressures, resulting in fragmentation across regions, countries, and sectors (Nambisan & Luo, 2021). While Luo (2022b) refers to the roots of data localization measures as grounded in new 'techno-nationalism', his focus is primarily on the ideologies pursued rather than the policies themselves. Luo and Van Assche (2023) discuss heightened techno-geopolitical uncertainties stemming from policy initiatives in relation to the United States (US) CHIPS and Science Act, thus focusing on one specific industry.

We propose that all these aspects are part of a larger puzzle that demands holistic investigation, taking into account the distinct laws, interests, and human rights involved. Given the differences in data intensity and public scrutiny between sectors, it seems worthwhile to start with exploratory, qualitative (industry case) studies. A more detailed understanding of data governance would not only facilitate a nuanced comprehension of implications for MNEs and IB, but also promote a bi-directional dialogue between the IB community and policymakers on data and digitalization issues. The text and tables below differentiate between the regulatory challenges across countries governing respectively the **use, transfer, storage** and **flows** of data, as well as between policies concerning **personal** and/or **non-personal** data. It is important to note that, given the numerous laws currently under discussion at the EU level that build upon the ones we examine, the list below is not exhaustive and is primarily intended to encourage IB scholars to further explore these issues (Tables 1, 2, 3 4).

Unlike non-personal data, which primarily concerns their re-use in a data-sharing context, the lawful **use** (i.e., processing) of personal data forms the core of the GDPR. As previously mentioned, this leads to significant variations globally and within the EU. While IB scholars observe that this results in MNEs facing the choice to "either follow the most stringent regulations everywhere at the risk of local competitive disadvantage or to divaricate regionally at the risk of creating governance approaches that are inconsistent across markets" (George & Schillebeeckx, 2022, p. 2), such a statement overlooks the potential impact of the Brussels effect, as well as the regulatory challenges across countries within regions (e.g., between EU Member States).

Concerning the former, Bradford's influential findings suggest that MNEs are likely to adopt GDPR standards globally. However, given the heterogenous effects of regulation (Peukert et al., 2022), we posit that such findings could vary depending on the firm in question, such as large versus small firms (Kuo, 2021), the countries targeted (emerging versus developed), and the timing of the exploration, with Bradford (2021) indicating that the Brussels effect could weaken over

Table 1 Regulatory challenges across countries related to the *usage* of data

	Personal data	Non-personal data
Variations between EU Member States	• Variation in terms of implementation, interpretation and enforcement.	Governance of non-personal data primarily concerns its re-use, instead of its primary use. Since re-use of data implies sharing it, this section is covered under "flows of data" (Table 4)
Regional variations	• "Open" (e.g., the US) • "Conditional" (e.g., the EU). • "Limited" (e.g., China).	
IB Implications	• Whether MNEs adapt their offering from one jurisdiction to another or take measures that comply with the strictest of the derogations (Brussels effect). • International trade implications (positive associations for countries sharing the "conditional" model).	

time, thereby implying room for longitudinal studies. The need to further delve into these aspects of data governance was recently confirmed by Peukert et al. (2022), who provided the first empirical evidence of the GDPR's Brussels effect on website providers. By noting other privacy regulations such as the CCPA that came into effect after their study[3] and have extraterritorial effects somehow similar to the GDPR, their work paves the way for further explorations of the Brussels effect.

In addition to regulatory divergence leading to compliance issues, MNEs also face variations in privacy perceptions (Mohammed & Tejay, 2017), which relate to the culturally rooted issue of data ethics (Hasselbalch, 2019). In his study exposing the manipulative data practices of tech companies, Waldman (2021) highlights firms' need to distinguish between compliance with data privacy laws and compliance with the values these laws serve. In that regard, a 2022 McKinsey report emphasizes companies' common misunderstanding about the relationship between data ethics and data laws, with the former extending beyond the latter (Edquist et al., 2022). While the GDPR encourages firms to engage with data ethically, the ethical use of data is context-dependent and relies on competing conceptions of 'right' and 'wrong' (Hijmans & Raab, 2018), which may prompt MNEs to supplement their standardized data privacy policies with country-specific corporate social responsibility practices or *vice versa* (Bamiatzi et al., 2023). The growing need for IB scholars to explore social imperatives in the digital era has been suggested in relation to both 'going digital' MNEs (Srinivasan & Eden, 2021), and multinational platforms faced with so-called 'ecosystem social responsibilities', also with respect to data privacy (Yi et al., 2023).

In terms of regulatory variations within regions, these could extend the Brussels effect by creating dilemmas for MNEs to either fine-tune compliance to each Member State's national laws or adopt a uniform approach, as TikTok did regarding minors' data (ICO, 2023). Concerning national variations in GDPR enforcement, the 2019 French Google case (CJEU, 2019) illustrates how this could influence MNEs' choice of main EU establishment, which is the 'one-stop-shop' provision that prevents companies from being prosecuted in every Member State in which they operate (Arnbak & Potjewijd, 2019). At that time, Google had its headquarters in Ireland but had not yet appropriately designated that country as its main establishment, allowing various national data protection authorities to prosecute the company. Another crucial IB implication concerns international trade in digital services, with indications that countries sharing the conditional model are positively associated with trade, compared to those adopting an open or limited one (Ferracane & Van der Marel, 2021).

Regarding data **transfers** (see Table 2), it is worth noting that most firms process mixed datasets containing both personal and non-personal data (European Commission, 2019). The fact that EU lawmakers are currently establishing separate data transfer regimes for each type of data raises concerns for Europe's digital growth, with IB implications expected to exacerbate those experienced so far concerning personal data due to increased uncertainties (Propp, 2022b). Consequently, the *Schrems II* effects are likely to intensify, with smaller firms, data-intensive sectors, and non-European cloud service providers particularly at risk (Mine & Bonefeld-Dahl, 2021; Propp, 2022b). At the same time, an impact survey (Bonefeld-Dahl et al., 2020) exposes how personal data transfer policies affect all industries and firms, therefore extending beyond MNEs. For example, data transfer issues in the TikTok case caused public organizations, including EU institutions and the French government, to limit their employees access to the app (Euronews, 2023; Le Monde, 2023). Whereas the former prohibited its staff from installing TikTok on their work devices, the latter went a step further

[3] Their study is based on pre-GDPR data (12 months before it came into force) and post-GDPR data (6 months after it came into force). The CCPA came into force in January 2020.

Table 2 Regulatory challenges across countries related to the *transfer* of data

	Personal data	Non-personal data
Variations between EU Member States	Not applicable as these concern data flows to third countries or multinational enterprises whose mechanisms are decided at the EU level.	
Regional variations	Different conditions as to whether or not data can be transmitted beyond country borders, based on data privacy and data security considerations (EU: third country must offer an 'adequate level of protection'). • "Open" (e.g., Australia; Mexico; the US). • "Conditional" (e.g., Argentina; the EU, Singapore; Turkey). • "Limited" (Brunei; China; Russia; Tunisia).	• Different conditions as to whether or not data can be transmitted beyond country borders, based on trade secrets and IPR protection (EU: 'third country must offer an 'adequate level of protection').
IB Implications	• Deglobalization of supply chains & international trade implications (positive associations for countries sharing an "open" model). • Setting up of foreign subsidiaries entrusted with core functions related to national security concerns. • Reconfiguration of headquarter–subsidiary relationships to contain data transfers. • Employment of local staff to oversee data transfers. • MNEs' choice to leave certain markets.	• Strengthen IB effects *vis-à-vis* personal data (because of increased uncertainty). • Particularly likely to hit the manufacturing industry by disincentivizing exports of EU technologies.

by banning all recreational applications, such as Netflix, Instagram, and Candy Crush. Meanwhile, the list of countries either fully or partially banning TikTok, such as Australia, India, and the US, is rapidly increasing (Sweney, 2023). This sheds light on data transfers being at stake in a wide range of day-to-day situations, from "manufacturers supporting their customers overseas" to firms having "employees in multiple countries" or companies "incorporating advanced data analytics and machine learning methods into their services" (Bonefeld-Dahl et al., 2020, p. 5).

In the digital age, data flows are an intrinsic part of value chains, with outsourcing activities forming the biggest part of firms' data transfers. Hence, the main implications of cross-country variations in that sphere are likely to concern firms' selection of business partners, and, therefore, a reconfiguration of their value chains. It can impact their choice of cloud service providers (Claburn, 2022; Lomas, 2022), as well as their reliance on third-party services such as Google Analytics[4] (Denis, 2022; DSB, 2021). More drastically, data transfer limitations could also incentivize firms to withdraw from certain countries. As Meta declared in the aftermath of *Schrems II*: "if we are unable to transfer data between and among countries and regions in which we operate, or if we are restricted from sharing data among our products and services, it could affect our ability to provide our services" (United States Securities & Exchange Commission, 2022). In China, Nike withdrew its popular Run Club App from the market to "create an ecosystem from China for China" (Liang & Kubota, 2022). Similarly, a 2022 report illustrates how the EU 'legal maze' could disincentivize European firms, both cloud service providers and traditional firms, from entering or staying in foreign markets (Bonefeld-Dahl, 2022).

In addition to the increased focus on deglobalization, IB scholars should also consider foreign firms' strategies to enter or retain host markets with strict data transfer policies in place. In China, LinkedIn transformed its services into InCareer to bypass data export regulations (Taojun et al., 2023). Unlike the Western version, this Chinese-tailored platform does not allow any social feeds or post-sharing features. Relatedly, to continue operating in the US, TikTok created a new subsidiary called 'TikTok US Data Security Inc.', governed by an independent board of directors and employing only US citizens or green card holders (Perault & Sacks, 2023). Additionally, it appointed a US-based cloud service provider to oversee data flows and ensure they do not pose risks to national security. Similarly, in Europe, TikTok announced external oversight of its data flows by a European third party (Bertram, 2023). Concerning international trade, it appears that countries sharing an open data transfer model are more likely to trade together, as opposed to countries sharing a limited approach (Ferracane & Van der Marel, 2021)

[4] In July 2022, the French Data Protection Authority found the data transfers by Google in the context of its data analytics services provided to EU websites unlawful as they do not sufficiently preclude data access by US intelligence services under 50 US. Code § 1881a ("FISA 702").

Table 3 Regulatory challenges across countries related to the *storage* of data

	Personal data	Non-personal data
Variations between EU Member States	• France has recently introduced mandatory data localization requirements for cloud service providers used by public entities ("Trusted Cloud Doctrine").	Not applicable: Data localization laws are prohibited since the Regulation on the free flow of non-personal data in the EU.
Regional variations	• Variations regarding whether and, if so, how data must be stored locally. The EU does not (yet) "formally" impose data localization requirements on personal data. • Certain countries have data localization requirements in place, without distinguishing between personal or non-personal data (e.g., China requires "important business data" to be stored there [Cyber Security law]). • "Open" (e.g., Mexico; New Zealand). • "Conditionally open" (e.g., Sweden). • "Conditionally closed" (e.g., Australia). • "Limited" (e.g., China; Indonesia).	
IB Implications	• Impacts the IT infrastructure/technologies used by MNEs to store their data (e.g., cloud-based datacenters; colocation datacenters; on-premise infrastructures). • The building of local datacenters by cloud service providers (using particular ownership & partnership structures). • MNEs' choice to leave certain markets.	

Data **storage** policies have led many MNEs to set up local facilities and/or switch to local cloud service providers. These operational changes are usually accompanied by significant organizational changes, with requirements for local staff to oversee data flows and foreign data access, tasks not typically dealt with at the subsidiary level (cf. Cory, 2021). Again, the TikTok case illustrates operational changes, as the company plans to migrate EU citizens' data to co-location sites in Ireland and Norway (Bertram, 2023) and rely on US-based Oracle Cloud servers for US users' data storage (Baker-White, 2022). Some MNEs establish inventive data storage partnerships to navigate conflicting data storage policies, such as Apple's partnership with the Chinese firm Guizhou-Cloud Big Data (GCBD). This partnership made GCBD the legal owner of locally stored data, by which "Chinese authorities can demand access to data from GCBD rather than Apple, and the terms shield Apple from legal reprisal in the US" (Mozur et al., 2017; Peterson, 2021). Similarly, in 2017, Amazon Web Services announced a partnership with a Chinese firm to ensure compliance with local regulations (Reuters, 2017). Within the EU, Google Cloud developed a co-ownership model with the French company Thales to obtain the 'trusted cloud label' following France's 2021 sovereign cloud strategy (Dataguidance, 2021; République Francaise, 2021; Thales, 2021).

Given the costs of setting up local data storage facilities, the way MNEs deal with data storage policies seems to differ among countries and may depend on factors such as firm size (Chander, 2020) and type of industry (Kennedy-Mayo & Swire, 2021). A 2022 survey reveals that digital sovereignty and compliance considerations have broader implications for firms' IT architecture, namely its design, operation, and management (IDC, 2023). Therefore, how MNEs choose to adopt cloud facilities, invest in data storage infrastructure, adopt a mixed approach, or cease their activities within a given country is an interesting IB dilemma. The PayPal case, where the company discontinued operations in Turkey due to data localization requirements, demonstrates the far-reaching consequences of these policies: "PayPal utilizes a global payments platform that operates across more than 200 markets, rather than maintaining local payments platforms with dedicated technology infrastructure in any single country" (Lunden, 2016).

Data **flow** policies, on the other hand, are primarily innovation-driven and therefore expected to affect firms' digital transformation as they strive to become more inventive. With data-sharing frameworks still being shaped at the EU level, much of their implications on MNEs remain to be discovered (cf. Table 4). In the banking sector, data-sharing obligations under PSD2 have already had a noticeable impact on firms, which started to innovate their business models by means of application programming interface (API) technologies and collaborations, giving rise to new ecosystems and platforms (Omarini, 2018; Ozcan & Zachariadis, 2021; Radnejad et al., 2021). Such regulatory initiatives also seem to trigger an unbundling of value chains, whereby a shift from a horizontal to a vertical banking industry occurs (Ozcan & Zachariadis, 2021).

Cross-country intricacies in data flow policies primarily affect MNEs' digital transformation, with variations expected depending on the country and firm at stake (Petrović, 2020). Given that each country shapes, through its own regulatory framework, the tension between data innovation, on the one hand, and data privacy/security, IPR and trade secrets, on the other, MNEs' main challenge resides in their ability to transform while respecting conflicting interests, which may strengthen the 'loose coupling' view suggested by Nambisan and Luo (2021). Consequently, MNEs need to strategize to overcome cognitive barriers and strike a balance between openness and control, with openness

Table 4 Regulatory challenges across countries related to the *flows* of data

	Personal data	Non-personal data
Variations between EU Member States	• Variations in interpretation and implementation of interoperability and security standards under PSD2.	• Variations in implementation of the Open Data Directive (concerns public sector information data and publicly-funded research data).
Regional variations	• Variations in terms of scope of data (open banking vs. open finance) • Variations in the ways data-sharing should occur (e.g., through standardized APIs [UK] or not [EU]). • Prescriptive (e.g., Australia; the EU; the UK). • Facilitative (e.g., Hong Kong; Japan; Singapore). • Market-driven (e.g., China; the US). • Regulatory–industry driven (e.g., sharing obligations and actors concerned (e.g., Canada).	• Variations in scope of data-sharing obligations and actors concerned (e.g., unlike most jurisdictions, the DGA and DA extend data-sharing obligations beyond publicly-held data).
IB Implications	• Impacts the way in which MNEs digitally transform (e.g., development of new business models and ecosystems; development of new data-driven based products). • Faces MNEs with the challenge to innovate and build ecosystems whilst minimizing societal risks (innovation vs. data privacy; innovation vs. trade secrets & IPR).	

involving both business and societal risks (Volberda et al., 2021).

Data-sharing increases business risks such as regulatory complexity, cybersecurity vulnerabilities and digital interdependence (Luo, 2022a). The societal dimensions of these risks, such as data privacy harms, are context-dependent, making responsible transformation through data-sharing a challenging task for MNEs. This complexity becomes more pronounced in the context of emerging players such as 'data aggregators', which are increasingly being relied upon by many financial firms for their cross-border operations, digitalization strategies, and international expansion efforts but whose business models carry significant data privacy and security risks (Awrey & Macey, 2023). The affordance perspective, which highlights the 'bright' and 'dark' sides of digitalization, can be useful for MNEs to strategize and deploy their digital technologies in a way that serves sustainable development goals (Ciulli & Kolk, 2023). Focusing on the societal dimension of MNEs' digital transformation within certain geopolitical contexts would also respond to calls by management scholars (Dąbrowska et al., 2022) and contribute to a better understanding of why national contexts still matter in the digital age (Meyer et al., 2023). IB policy researchers can play an important role in helping policymakers and MNEs in better achieving their intended objectives.

The fragmentation of regulations at global, regional, and even domestic levels—a complication particularly pronounced in data-sharing contexts due to the layered complexities and interrelationships around data privacy and security frameworks—could be seriously reduced through a coherent international data governance framework. Moving in this direction seems critical given the growing number of regulations worldwide promoting data-sharing within and across sectors, such as the EU's current exploration of transitioning from an 'open banking' to an 'open finance' framework. Thus, while we concur with the observation that "traditional institutional frameworks are no longer adapted to effectively keep up with these policy challenges, as they only have limited effectiveness" (OECD, 2023, p. 23), cross-border and cross-sectoral regulatory cooperation in pursuit of shared approaches might help to reduce complexity. The very 'Brussels effect' sparking comparable rule-setting outside the EU can help pave the way as well.

Organizations such as the OECD Working Party on Data Governance and Privacy in the Digital Economy might be instrumental in such processes. For instance, in its commitment to guiding stakeholders towards regulatory cohesion, the OECD issued best practice principles on international regulatory cooperation in 2021, followed by a recommendation on regulatory cooperation for global challenges in 2022. These steps, at the very least, sparked international dialogue. In addition, recognizing the need to operationalize data governance frameworks, we underline the crucial role of MNEs in engaging with stakeholders and developing and sharing best practices among those actors facing similar challenges. The Berlin Group, a pan-European banking association that encompasses numerous industry players such as banks and payments associations, is an example. It played a key role in surmounting implementation hurdles posed by data-sharing laws by creating common open banking API standards, thereby fostering more secure and effective data exchange within the EU and among industry (Nocash, 2023). Involving firms in an early stage to discuss practicalities of (future) enactment and/or the feasibility of 'real-world' enforcement should not be confused with 'self-policing' or excessive lobbying to avoid regulation from happening. The latter is a well-known phenomenon but generally not considered a part of corporate digital or data responsibility.

Conclusion

This paper aimed to untangle the cross-country regulatory intricacies in data governance and to build upon existing IB studies that describe the situation as an "ever more complex, pluralistic institutional context" (George & Schillebeeckx, 2022, p. 2). Explicating insights from the legal field, and using illustrative examples, it demonstrated that national and regional variations in the use, transfer, storage and flows of data impact MNEs in distinct ways. We advocate for further exploration of the implications for IB with respect to both personal and non-personal data, as well as the balance between data protection and data innovation, which lingers through whatever policies are taken in this realm. A better understanding of the globally fragmented data governance landscape can also offer valuable insights into 'decoupling' or 'derisking', brought to the fore already for both the US and Europe in relation to China (Witt et al., 2023). We encourage IB scholars to further investigate the roots of decoupling/derisking, which, in our view, extend beyond economic, political, and technological drivers, to encompass societal drivers embedded in data governance laws. Both the *Schrems II* judgment and the DGA have data privacy and IPR protection at their core. With this in mind, our work aims to provide concrete insights into current regulatory challenges facing MNEs, and we hope to inspire IB (policy) scholars to conduct research in the data governance sphere that will both guide MNEs in becoming responsible global citizens from a human rights point of view (Doh et al., 2023), and assist policymakers in achieving their intended goals, which—in our view—would benefit from regulatory convergence at international levels.

References

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.

Arnbak, A., & Potjewijd, G. (2019). First big GDPR fine for Google: Implications for multinationals. Retrieved August 1, 2023, from https://www.debrauw.com/articles/first-big-gdpr-fine-for-google-implications-for-multinationals

Arner, D. W., Castellano, G., & Selga, E. (2022). The transnational data governance problem. *Berkeley Technology Law Journal, 37*, 623–700.

Asia, E. P. A. (2021). *Open Banking APAC—New world collaboration for payments*. EPA Asia.

Awrey, D., & Macey, J. (2023). The promise & perils of open finance. *Yale Journal on Regulation, 40*(1), 1–59.

Baker-White, E. (2022). Leaked audio from 80 internal TikTok meetings shows that US user data has been repeatedly accessed from China. Retrieved August 1, 2023, from https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

Bamiatzi, V., Dowling, M., Gogolin, F., Kearney, F., & Vigne, S. (2023). Are the good spared? Corporate social responsibility as insurance against cyber security incidents. *Risk Analysis*, 1–16.

Becker, R., & Henderson, V. (2000). Effects of air quality regulations on polluting industries. *Journal of Political Economy, 108*(2), 379–421.

Bertram, T. (2023). Setting a new standard in European data security with Project Clover. Retrieved August 1, 2023, from https://newsroom.tiktok.com/en-eu/setting-a-new-standard-in-european-data-security-with-project-clover

Bertuzzi, L. (2022). EU Commission explains Data Act's legal implications to member States. Retrieved August 1, 2023, from https://www.euractiv.com/section/digital/news/eu-commission-explains-data-acts-legal-implications-to-member-states/

Boardman, R., Mullock, J., & Mole, A. (2020). *Guide to the general data protection regulation*. Bird & Bird.

Bodó, B., Irion, K., Janssen, H., & Giannopoulou, A. (2021). Personal data ordering in context: The interaction of meso-level data governance regimes with macro frameworks. *Internet Policy Review*. https://doi.org/10.14763/2021.3.1581

Bohnsack, R., Kolk, A., & Pinkse, J. (2015). Catching recurring waves: Low-emission vehicles, international policy developments and firm innovation strategies. *Technological Forecasting and Social Change, 98*, 71–87.

Bonefeld-Dahl, C. (2022). *Data transfers in the data strategy: Understanding myth and reality*. Digital Europe.

Bonefeld-Dahl, C., Heemskerk, F., Beyrer, M. J., & Huitema, E.-M. (2020). *Schrems II: Impact survey report*. Digital Europe.

Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review, 107*(1), 1–68.

Bradford, A. (2021). The European Union in a globalised world: The "Brussels effect." *Revue Européenne Du Droit, 2*(1), 75–79.

Brill, J., & Chapple, E. (2022). Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins. Retrieved August 1, 2023, from https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout

Brouthers, K. D., Chen, L., Li, S., & Shaheer, N. (2022). Charting new courses to enter foreign markets: Conceptualization, theoretical framework, and research directions on non-traditional entry modes. *Journal of International Business Studies, 53*(9), 2088–2115.

Bu, M., & Wagner, M. (2016). Racing to the bottom and racing to the top: The crucial role of firm characteristics in foreign direct investment choices. *Journal of International Business Studies, 47*(9), 1032–1057.

Buckley, R. P., Jevglevskaja, N., & Farrell, S. (2021). *Australia's data-sharing regime: Six lessons for the world*. No. 21–67.

Cha, H., Kotabe, M., & Wu, J. (2023). Reshaping internationalization strategy and control for global E-commerce and digital transactions: A Hayekian perspective. *Management International Review, 63*(1), 161–192.

Chander, A. (2020). Is data localization a solution for Schrems II? *Journal of International Economic Law, 23*(3), 771–784.

Ciulli, F., & Kolk, A. (2023). International Business, digital technologies and sustainable development: Connecting the dots. *Journal of World Business, 58*(4), 101445.

CJEU. (2015). *Judgment of the Court (Grand Chamber) of 6 October 2015: Maximillian Schrems v Data Protection Commissioner*. Luxembourg: Grand Chamber. Retrieved August 1, 2023, from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

CJEU. (2019). *Request for a preliminary ruling under Article 267 TFEU from the Conseil d'État: Google LLC v CNIL*. Luxembourg: Grand Chamber. Retrieved August 1, 2023, from https://curia.europa.eu/juris/document

CJEU. (2020). *Judgment of the Court (Grand Chamber) of 16 July 2020: Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Grand Chamber. Retrieved August 1, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311&qid=1627552758320

Claburn, T. (2022). France says non to Office 365 and Google Workspace in school. Retrieved August 1, 2023, from https://www.theregister.com/2022/11/22/france_no_windows_google/

Clegg, J. (2019). From the editor: International business policy: What it is, and what it is not. *Journal of International Business Policy, 2*, 111–118.

Cole, M. A. (2004). Trade, the pollution haven hypothesis and the environmental Kuznets curve: Examining the linkages. *Ecological Economics, 48*(1), 71–81.

Conseil d'Etat. (2020). Health Data Hub et protection de données personnelles: Des précautions doivent être prises dans l'attente d'une solution pérenne. Retrieved August 1, 2023, from https://www.conseil-etat.fr/actualites/health-data-hub-et-protection-de-donnees-personnelles-des-precautions-doivent-etre-prises-dans-l-attente-d-une-solution-perenne

Cory, N. (2021). Sovereignty requirements in France -and potentially EU- cybersecurity regulations: The latest barrier to data flows, digital trade, and digital cooperation among likeminded partners. Retrieved August 1, 2023, from https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/

Cui, V., Narula, R., Minbaeva, D., & Vertinsky, I. (2022). Towards integrating country- and firm-level perspectives on intellectual property rights. *Journal of International Business Studies, 53*(9), 1880–1894.

Cumming, D., Johan, S., Khan, Z., & Meyer, M. (2023). E-Commerce policy and international business. *Management International Review, 63*(1), 3–25.

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review, 34*(2), 234–243.

Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Giones, F., Hakala, H., Marullo, C., Mention, A-L., Mortara, L., Nørskov, S., Nylund, P. A., Oddo, C. M., Radziwon, A., Ritala, P. (2022). Digital transformation, for better or worse: A critical multi-level research agenda. *R&D Management*, *52*(5), 930–954.

Daigle, B., & Khan, M. (2020). The EU General Data Protection Regulation: An analysis of enforcement trends by EU data protection authorities. *Journal of International Commerce and Economics*, advance online publication June. https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf

DAMA International. (2009). *The DAMA guide to the data management body of knowledge* (1st ed.). Technics Publications.

Daniel, M. L. (2022). Argentina: The right to be forgotten strikes again. Retrieved August 1, 2023, from https://techpolicy.press/argentina-the-right-to-be-forgotten-strikes-again/

Data Protection Commission. (2021). DPC launches two inquiries into TikTok concerning compliance with GDPR requirements relating to the processing of childrens' personal data and transfers of data to China. Retrieved August 1, 2023, from https://www.dataprotection.ie/en/news-media/latest-news/dpc-launches-two-inquiries-tiktok-concerning-compliance-gdpr-requirements-relating-processing

Dataguidance. (2021). France: The new national cloud strategy—Data transfer and localization implications. Retrieved August 1, 2023, from https://www.dataguidance.com/opinion/france-new-national-cloud-strategy-data-transfers

Dataguidance. (2022). Privacy 101: Data protection impact assessment. Retrieved August 1, 2023, from https://www.dataguidance.com/resource/privacy-101-data-protection-impact-assessment

Denis, M.-L. (2022). Decision ordering the company to comply. *Commission Nationale Informatique & Libertés*. Retrieved August 1, 2023, from https://www.cnil.fr/sites/cnil/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf

Doh, J. P., Eden, L., Tsui, A. S., & Zaheer, S. (2023). Developing international business scholarship for global societal impact. *Journal of International Business Studies, 54*, 757–767.

DSB. (2021). Partial decision. Retrieved August 1, 2023, from https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf

Dyer, G. (2013). Snowden revelations stir up anti-US sentiment. Retrieved August 1, 2023, from https://www.ft.com/content/0ee001a0-eb13-11e2-bfdb-00144feabdc0

EDPB. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. Brussels.

EDPS. (2021). The EDPS opens two investigations following the "Schrems II" judgment. Retrieved August 1, 2023, from https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en

Edquist, A., Grennan, L., Griffiths, S., & Rowshankish, K. (2022). Data ethics: What it means and what it takes. Retrieved August 1, 2023, from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes

Euronews. (2023). Which countries have banned TikTok and why? Retrieved August 1, 2023, from https://www.euronews.com/next/2023/04/04/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears

European Commission. (2019). *Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*. Brussels, 29 May 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250.

European Commission. (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data*. Brussels, 19 February 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

European Commission. (2022a). Shaping Europe's digital future: Data Act – Factsheet. Retrieved August 1, 2023, from https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet

European Commission. (2022b). Data Act: Commission proposes measures for a fair and innovative data economy. Retrieved August 1, 2023, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

European Commission. (2022c). Shaping Europe's digital future: Data Governance Act explained. Retrieved August 1, 2023,

from https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained
Ferracane, M. F., & Van der Marel, E. (2021). *Regulating personal data: Data models and digital services trade*. Policy Research Working Paper, No. WPS 9596. World Bank Group.
George, G., & Schillebeeckx, S. J. D. (2022). Digital transformation, sustainability, and purpose in the multinational enterprise. *Journal of World Business, 57*(3), 101326.
Gestrin, M., & Staudt, J. (2018). *The digital economy, multinational enterprises and international investment policy*. OECD.
Hasselbalch, G. (2019). Making sense of data ethics. The powers behind the data ethics debate in European policymaking. *Internet Policy Review*. https://doi.org/10.14763/2019.2.1401
Heiber, J. G., & Workman, G. (2023). *The EU Data Act: A misguided policy*. US Chamber of Commerce.
Hennart, J.-F. (2019). Digitalized service multinationals and international business theory. *Journal of International Business Studies, 50*, 1388–1400.
Hijmans, H., & Raab, C. D. (2018). Ethical dimensions of the GDPR. In M. Cole & F. Boehm (Eds.), *Commentary on the general data protection regulation.* Edward Elgar.
ICO. (2023). ICO fines TikTok 12.7 million for misusing children's data. Retrieved August 1, 2023, from https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/
IDC. (2023). IDC survey finds data sovereignty and compliance issues shaping IT decisions. Retrieved August 1, 2023, from https://www.idc.com/getdoc.jsp?containerId=prUS50134623
Junck, R. D., Klein, B. A., Kumaki, A., Kumayama, K. D., Kwok, S., Levi, S. D., Talbot, J. S., Vermynck, E-C., Zhang, S. (2021). China's new Data Security and Personal Information Protection Laws: What they mean for multinational companies. Retrieved August 1, 2023, from https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws
Kennedy-Mayo, D., & Swire, P. (2021). New urgency about data localization with Portuguese decision. Retrieved August 1, 2023, from https://iapp.org/news/a/new-urgency-about-data-localization-with-portuguese-decision/
Kuo, M. A. (2021). The Brussels effect and China: Shaping tech standards. Retrieved August 1, 2023, from https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards/
Latham & Watkins. (2018). GDPR resource center—Derogations tracker. Retrieved August 1, 2023, from https://gdpr.lw.com/Home/Derogations
Le Monde. (2023). France bans TikTok from public employee work phones. Retrieved August 1, 2023, from https://www.lemonde.fr/en/politics/article/2023/03/24/france-bans-tiktok-from-public-employee-work-phones_6020523_5.html
Liang, R., & Kubota, Y. (2022). Nike to end run club app in China. Retrieved August 1, 2023, from https://www.wsj.com/articles/nike-to-end-run-club-app-in-china-11654698300
Lomas, N. (2022). Microsoft 365 faces darkening GDPR compliance clouds after German report. Retrieved August 1, 2023, from https://techcrunch.com/2022/11/28/microsoft-365-faces-darkening-gdpr-compliance-clouds-after-german-report/?guccounter=1
López González, J., Casalini, F., & Porras, J. (2022). *A preliminary mapping of data localisation measures*. OECD Trade Policy Papers, No. 262 (June). OECD Publishing.
Lundan, S., & Van Assche, A. (2021). From the editors: Reflections on the nexus of complementarity between international business research and the policy practitioner community. *Journal of International Business Policy, 4*(2), 201–205.
Lunden, I. (2016). PayPal to halt operations in Turkey after losing license, impacts 'hundreds of thousands'. Retrieved August 1, 2023, from https://techcrunch.com/2016/05/31/paypal-to-halt-operations-in-turkey-after-losing-license-impacts-hundreds-of-thousands/
Luo, Y. (2022a). A general framework of digitization risks in international business. *Journal of International Business Studies, 53*(2), 344–361.
Luo, Y. (2022b). Illusions of techno-nationalism. *Journal of International Business Studies, 53*(3), 550–567.
Luo, Y., & Van Assche, A. (2023). The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act. *Journal of International Business Studies*. https://doi.org/10.1057/s41267-023-00620-3
Madan, S., Savani, K., & Katsikeas, C. S. (2022). Privacy please: Power distance and people's responses to data breaches across countries. *Journal of International Business Studies, 54*, 731–754.
Marini, A., Kateifides, A., Bates, J., Zanfir-Fortuna, G., Bae, M., Gray, S., & Sen, G. (2020). *Comparing privacy laws: GDPR v. CCPA*. Future of Privacy Forum.
McGaughey, S. L., & Raimondos, P. (2019). Shifting MNE taxation from national to global profits: A radical reform long overdue. *Journal of International Business Studies, 50*, 1668–1683.
Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R.-J. (2023). International business in the digital age: Global strategies in a world of national institutions. *Journal of International Business Studies, 54*, 577–598.
Milkaite, I., & Lievens, E. (2019). Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU. Retrieved August 1, 2023, from https://www.betterinternetforkids.eu/practice/awareness/article?id=3017751#BE
Milmo, D. (2022). TikTok tells European users its staff in China get access to their data. Retrieved August 1, 2023, from https://www.theguardian.com/technology/2022/nov/02/tiktok-tells-european-users-its-staff-in-china-get-access-to-their-data
Mine, H., & Bonefeld-Dahl, C. (2021). *Data flows and the digital decade*. Digital Europe.
Mohammed, Z. A., & Tejay, G. P. (2017). Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. *Computers & Security, 67*, 254–265.
Molina, O. (2018). Personal data protection is a constitutional right in Chile. Retrieved August 1, 2023, from https://iapp.org/news/a/personal-data-protection-is-a-constitutional-right-in-chile/
Monaghan, S., Tippmann, E., & Coviello, N. (2020). Born digitals: Thoughts on their internationalization and a research agenda. *Journal of International Business Studies, 51*, 11–22.
Mozur, P., Wakabayashi, D., & Wingfield, N. (2017). Apple opening data center in China to comply with cybersecurity laws. Retrieved August 1, 2023, from https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html
Nambisan, S. (2022). Digital innovation and international business. *Innovation, 24*(1), 86–95.
Nambisan, S., & Luo, Y. (2021). Toward a loose coupling view of digital globalization. *Journal of International Business Studies, 52*, 1646–1663.
Nambisan, S., Zahra, S. A., & Luo, Y. (2019). Global platforms and ecosystems: Implications for international business theories. *Journal of International Business Studies, 50*, 1464–1486.
Nocash. (2023). Berlin group is offering support to new European payment schemes. Retrieved August 1, 2023, from https://nocash.ro/berlin-group-is-offering-support-to-new-european-payment-schemes/
NOYB. (2023). European Commission gives EU-US data transfers third round at CJEU. Retrieved August 1, 2023, from https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

Ocelík, V., & Kolk, A. (2023). Sustainability in a digital world: Geopolitics, values and international business policy. In P. Gugler & A. T. Lehmann (Eds.), *Handbook of international business policy.* Edward Elgar Publishing.

Ocelík, V., Kolk, A., & Ciulli, F. (2023). Multinational enterprises, Industry 4.0 and sustainability: A multidisciplinary review and research agenda. *Journal of Cleaner Production, 413*, 137434.

OCI. (2023). European Union Restricted Access (EURA) and SaaS Security. Retrieved August 1, 2023, from https://www.oracle.com/security/saas-security/data-sovereignty/european-union-restricted-access/

OECD. (2021). *OECD best practice principles for regulatory policy: International regulatory co-operation*. OECD Publishing.

OECD. (2023). *Data portability in open banking: Privacy and other cross-cutting issues*. OECD.

OECD Council. (2022). Recommendation of the Council on international regulatory co-operation to tackle global challenges. Retrieved August 1, 2023, from https://www.oecd.org/mcm/Recommendation-on-International-Regulatory-Co-operation-to-Tackle-Global-Challenges.pdf

Ohab, D., & Shariff, S. (2023). Open banking in Canada: The path forward. Retrieved August 1, 2023, from https://www.ey.com/en_ca/banking-capital-markets/open-banking-in-canada-the-path-forward

O'Hara, K., & Hall, W. (2018). *Four internets: The geopolitics of digital governance*. Centre for International Governance Innovation.

Omarini, A. E. (2018). Banks and Fintechs: How to develop a digital open banking approach for the bank's future. *International Business Research, 11*(9), 23–36.

Ozcan, P., & Zachariadis, M. (2021). *Open Banking as catalyst for industry transformation: Lessons learned from implementing PSD2 in Europe*. Swift Institute Working Paper, No. 2017 (September). The Swift Institute.

Perault, M., & Sacks, S. (2023). Project Texas: The details of TikTok's plan to remain operational in the United States. Retrieved August 1, 2023, from https://www.lawfareblog.com/project-texas-details-tiktoks-plan-remain-operational-united-states

Peterson, M. (2021). Report details security compromises Apple had made to placate China. Retrieved August 1, 2023, from https://appleinsider.com/articles/21/05/17/report-details-security-compromises-apple-has-made-to-placate-china

Petrović, M. (2020). PSD2 influence on digital banking transformation: Banks' perspective. *Journal of Process Management New Technologies, 8*(4), 1–14.

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

Pisani, N., Kolk, A., Ocelík, V., & Wu, G. (2019). Does it pay for cities to be green? An investigation of FDI inflows and environmental sustainability. *Journal of International Business Policy, 2*(1), 62–85.

Propp, K. (2022a). European cybersecurity regulation takes a sovereign turn. Retrieved August 1, 2023, from https://www.crossborderdataforum.org/european-cybersecurity-regulation-takes-a-sovereign-turn/

Propp, K. (2022b). The EU's proposed Data Act: Regulating international flows of non-personal data. Retrieved August 1, 2023, from https://www.crossborderdataforum.org/the-eus-proposed-data-act-regulating-international-flows-of-non-personal-data/

Radnejad, A. B., Osiyevskyy, O., & Scheibel, O. (2021). Learning from the failure of the EU Payments Services Directive (PSD2): When imposed innovation does not change the status quo. *Rutgers Business Review, 6*(1), 79.

République Francaise. (2021). *Circulaire n. 6282-SG Du 5 Juillet 2021 Relative a La Doctrine d'utilisation de l'informatique En Nuage Par l'Etat. République Francaise*. Paris, 5 July 2021. https://www.legifrance.gouv.fr/download/pdf/circ?id=45205

Reuters. (2017). Amazon's cloud unit expands in China, with new partner in Ningxia. Retrieved August 1, 2023, from https://www.reuters.com/article/us-china-amazon-idUSKBN1E60CN

Samiee, S. (1984). Transnational data flow constraints: A new challenge for multinational corporations. *Journal of International Business Studies, 15*(1), 141–150.

Srinivasan, N., & Eden, L. (2021). Going digital multinationals: Navigating economic and social imperatives in a post-pandemic world. *Journal of International Business Policy, 4*, 228–243.

Stastny, J. (2022). Open Banking in Europe in light of PSD2 review. Retrieved August 1, 2023, from https://www.kinstellar.com/news-and-insights/detail/1611/open-banking-in-europe-in-light-of-psd2-review

Stauss, D., & Weber, S. (2022). How do the CPRA, CPA & VCDPA treat publicly available information? Retrieved August 1, 2023, from https://www.bytebacklaw.com/2022/01/how-do-the-cpra-cpa-vcdpa-treat-publicly-available-information

Sweney, M. (2023). European Commission bans staff using TikTok on work devices over security fears. Retrieved August 1, 2023, from https://www.theguardian.com/technology/2023/feb/23/european-commission-bans-staff-from-using-tiktok-on-work-devices

Taojun, X., Jingting, L., Sengstschmid, U., & Yixuan, G. (2023). Navigating China's new cross-border data transfer rules. Retrieved August 1, 2023, from https://lkyspp.nus.edu.sg/docs/default-source/aci/thebusinesstimes_21feb2023_navigating-china-s-new-cross-border-data-transfer-rules.pdf

Tatarinov, K., Ambos, T. C., & Tschang, F. T. (2022). Scaling digital solutions for wicked problems: Ecosystem versatility. *Journal of International Business Studies, 54*, 631–656.

Thales. (2021). Thales and Google Cloud announce strategic partnership to jointly develop a trusted cloud offering in France. Retrieved August 1, 2023, from https://www.thalesgroup.com/en/group/investors/press_release/thales-and-google-cloud-announce-strategic-partnership-jointly

Tung, R. L. (2023). To make JIBS matter for a better world. *Journal of International Business Studies, 54*, 1–10.

UNCTAD. (2021). *Cross-border data flows and development: For whom the data flow*. United Nations.

UNCTAD. (2023). Data protection and Privacy legislation worldwide. Retrieved August 1, 2023, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

United States Securities and Exchange Commission. (2022). *Quarterly report pursuant to Section 13 OR 15(d) of the Securities Exchange Act of 1934*. Washington, D.C.

Vardanyan, L., & Kocharyan, H. (2022). The GDPR and the DGA proposal: Are they in controversial relationship? *European Studies, 9*(1), 91–109.

Vasylyk, O. (2022). Weekly digest April 4–10, 2022: EU data governance, digital products security, US law enforcement outreach & privacy. Retrieved August 1, 2023, from https://techgdpr.com/blog/weekly-digest-11042022-eu-data-governance-digital-products-security-us-law-enforcement-outreach/

Vogel, D. (1997). Trading up and governing across: Transnational governance and environmental protection. *Journal of European Public Policy, 4*(4), 556–571.

Vogelezang, F. 2022. The Data Act: Five implications for the datasphere. Retrieved August 1, 2023, from https://www.thedatasphere.org/news/the-data-act-five-implications-for-the-datasphere/

Volberda, H. W., Khanagha, S., Baden-Fuller, C., Mihalache, O. R., & Birkinshaw, J. (2021). Strategizing in a digital world: Overcoming cognitive barriers, reconfiguring routines and introducing new organizational forms. *Long Range Planning, 54*(5), 102110.

Von der Leyen, U. (2022). Dear honourable member. Retrieved August 1, 2023, from https://twitter.com/BrendanCarrFCC/status/1595057701695922176/photo/1

Waldman, A. E. (2021). *Industry Unbound: The inside story of privacy, data and corporate power*. Cambridge University Press.

Witt, M. A., Lewin, A. Y., Li, P. P., & Gaur, A. (2023). Decoupling in international business: Evidence, drivers, impact, and implications for IB research. *Journal of World Business, 58*(1), 101399.

Wu, E. (2021). *The cyber project: Sovereignty and data localization*. Belfer Center for Science and International Affairs.

Wu, X., & Gereffi, G. (2018). Amazon and Alibaba: Internet Governance, business models, and internationalization strategies. In A. Verbeke, R. Van Tulder, & L. Piscitello (Eds.), *International business in the information and digital age. Progress in international business research* (Vol. 13, pp. 327–356). Emerald Publishing Limited.

Yi, J., Li, J., & Chen, L. (2023). Ecosystem social responsibility in international digital commerce. *Journal of International Business Studies, 54*, 24–41.

Zygmuntowski, J. J., Zoboli, L., & Nemitz, P. F. (2021). Embedding European values in data governance: A case for public data commons. *Internet Policy Review*. https://doi.org/10.14763/2021.3.1572

Eugénie Coche is a doctoral candidate at the Amsterdam Business School, University of Amsterdam, the Netherlands. Her research interests lie at the intersection between law and international business, with a particular focus on the business and societal implications of digitalization policies. Central to her current project, funded by ABN AMRO, is exploring the tension between data privacy, security, and innovation.

Ans Kolk is Full Professor at the University of Amsterdam, Amsterdam Business School. Her areas of expertise are in corporate social responsibility, sustainable development, and sustainability, especially in IB. One stream of research, on which she has published in business and interdisciplinary outlets, involves the societal and environmental implications of digitalization and novel data-based technologies. For more information, see http://www.anskolk.eu.

Václav Ocelík is a doctoral candidate at the Amsterdam Business School, University of Amsterdam, the Netherlands. His research interests include corporate political activity, digitalization, and sustainability. Central to his research is understanding how corporations navigate and respond to regulations within the European Union.