Intangible Protectionism: When Firms Support Data Protection Regulation

Matteo Nebbiai

DRAFT – Please do not share

Abstract

The common narrative of digital trade politics portrays companies favouring free data flows and opposing government regulations constraining them. However, anecdotal evidence and survey data reveal that some firms actively support restrictions on data flows. How can this be explained? This paper argues that firms endorse stricter data regulations when such measures disproportionately increase costs for their foreign competitors. When data protection provisions impose asymmetric costs - raising barriers for foreign firms more than for domestic ones - domestic companies are incentivized to support these initiatives, anticipating gains in market share or profitability. I refer to this phenomenon as intangible protectionism.

To test this theory, I analyze public consultations related to the European Union's proposal to strengthen data protection requirements for firms storing European data outside the EU. A quantitative analysis of firms' preferences demonstrates that EU-based companies - facing lower adjustment costs relative to their foreign competitors - are significantly more likely to support these provisions, even after controlling for firm size, sector, and data vulnerability. Further, I examine the firms' reactions to a proposed "sovereign requirement" within an EU cybersecurity certification scheme, providing additional evidence for this mechanism.

This paper contributes to the literature on the politics of regulation in an increasingly intangible-intensive economy. It shows how data regulation can serve as a strategic tool for firms to advance protectionist objectives. Finally, it enriches the literature on interest groups by theorizing the emergence of "baptists and bootleggers" coalitions between firms and privacy-conscious governments or consumer associations.

1. Introduction

The common narrative of digital trade politics portrays companies favouring free data flows and opposing government regulations constraining them. According to this view, companies oppose (and lobby against) any regulation hindering the flow of data between countries. For instance, American Big Tech companies supported provisions in Free Trade Agreements that would limit governments' capacity to restrict cross-border data flows (Wallach, 2025).

However, some businesses seem to support restrictive data regulation. When the Indian government drafted a data protection law in 2019, some companies from the Indian tech industry expressed support towards data localisation measures (iSPIRTs, 2017). Companies from the European defence and space industry called for introducing data localisation requirements in an EU cloud cybersecurity certification scheme (ASD, 2024). Mukesh Ambani, one of the most prominent Indian businessmen, stated "In this new world, data is the new oil... India's data must be controlled and owned by Indian people and not by corporates, especially global corporations". How can this be explained?

In this paper, I argue that firms endorse stricter data regulation when it imposes significantly higher costs on their foreign competitors. When data protection provisions increase costs for businesses in a *homogeneous* way (across domestic and foreign companies), business is united in opposing them. When data protection provisions increase costs in a *heterogeneous* way (increasing costs for foreign companies in a disproportionate manner), domestic companies are more likely to support such initiatives, because they might increase their market share or profits. I call this *intangible protectionism*.

I empirically test this mechanism by analyzing survey data from public consultations on the European Union's Data Act, which proposed stricter data protection requirements for firms storing data outside the EU. A quantitative analysis of firms' preferences shows that EU-based companies – that suffer a lower cost of adjustment in comparison with their foreign competitors - are significantly more likely to support such provisions. Such results remain valid even when controlling for firms' size, sector and firm's data vulnerability.

This paper contributes to the debate on the politics of regulation in an increasingly intangible-intensive economy. Specifically, it demonstrates how data regulation can be employed by firms as a tool to pursue protectionist objectives. Also, it enriches the literature on interest groups by theorizing the emergence of "baptists and bootleggers" coalitions between firms and privacy-conscious governments or consumer associations.

In the second section, I review the literature on firms' preferences for cross-border data flows. In the third section, I elaborate on a theory of how heterogeneous adjustment costs of regulation can make some firms supportive of data protection measures. In the fourth and fifth sections, I illustrate quantitative and qualitative evidence supporting such a thesis. In the conclusions, I examine the theoretical implications emerging from these results.

2. Literature Review

Conventional wisdom suggests that the rise of the digital economy, characterized by the flow of data across different countries, is an inherently globalising force. This view was popularised by theorists of the Internet as a land detached from states, where free markets could flourish, untamed by government control, and accelerate the "flattening" of trade between developed and developing countries (Lehdonvirta, 2022). According to this view, (digital) globalisation is a win-win for everyone, and trade barriers will be lowered by a coalition of companies, states and consumers (Baldwin, 2016).

This view has been criticized and discredited by many events. States have developed concerns regarding the flow of data out of their borders, related to consumer protection (Greenleaf, 2021) and weaponisation against the state or national companies (Beaumier et al., n.d.). Meanwhile, consumers have increasingly expressed concern about how their data are used, despite the tension with their enjoyment of many low-cost digital services (Culpepper & Thelen, 2020). Hence, an increasing number of governments are restricting cross-border data flows, for instance by adopting data protection and data localisation provisions (Ferracane et al., 2018; OECD, 2020)

In this context, firms are often considered as consistently pursuing a pro-openness position. Since businesses have an interest in extracting data from users anywhere they can, they will oppose costly impediments such as data protection or localisation requirements (Weymouth, 2023, pg. 44). Even companies without data-intensive business models seem generally pro-openness because purchasing digital services or using digital platforms involves exchanging data across borders. Such positions have been repeatedly expressed by tech-focused business associations such as the American Chamber of Commerce, CCIA and DIGITALEUROPE.

Then, why do some firms support a stricter control of data flows? Emerging literature in political science and international political economy deals with cases of firms lobbying in support of stricter regulation. Gulotty's (2020) theory of "regulatory protectionism" shows that highly-productive MNCs support stricter regulation when it harms smaller and less-productive competitors, that are forced out of the market. Kennard (2020) has shown that, when environmental regulation is proposed, the heterogeneity of adjustment costs can make low-adjustment-cost firms supportive of the rules. This happens because regulation forces high-adjustment-cost competitors to drop part of their market share to low-adjustment-cost firms. Can some of these insights be applied to data regulation?

3. Theory

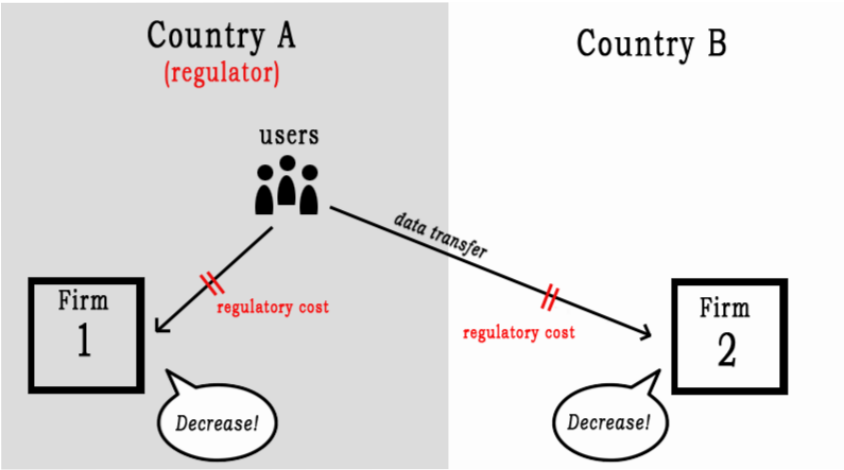
First, it is necessary to introduce what is the nature of compliance costs in the digital economy. Economic literature has stressed how one of the distinctive features of the digital economy is that the marginal cost of

duplicating and transferring intangibles such as data tends to be zero (Haskel & Westlake, 2018).[1] However, public regulation introduces new costs: some are fixed (i.e. drafting data protection risk assessments, establishing internal administrative routines), and some are variable (i.e. renting localised data servers, training new employees). Also, some regulations create risks such as data access requests by governments or trade secret leaks, that can be costly in terms of litigation or reputational damage (Crasnic et al., 2017).

Hence, regulation introduces a positive marginal cost of data production and distribution. This cost is the combination of many different variables, both related to the substance of legal provisions and internal operations of firms. Firms differ in the data intensity of their business, their capacity to monetise data, the locations where they store and analyse data, etc. The variation of these features makes the impact of any data regulation *heterogeneous* across firms. Following Kennard (2020), my claim is that this variation in firms' anticipated regulatory costs generates support or opposition. While many of these characteristics are not easy to investigate and their interaction with regulation is hard to foresee, there is a feature that is easy to observe and directly connected to the heterogeneous costs imposed by data regulation: location.

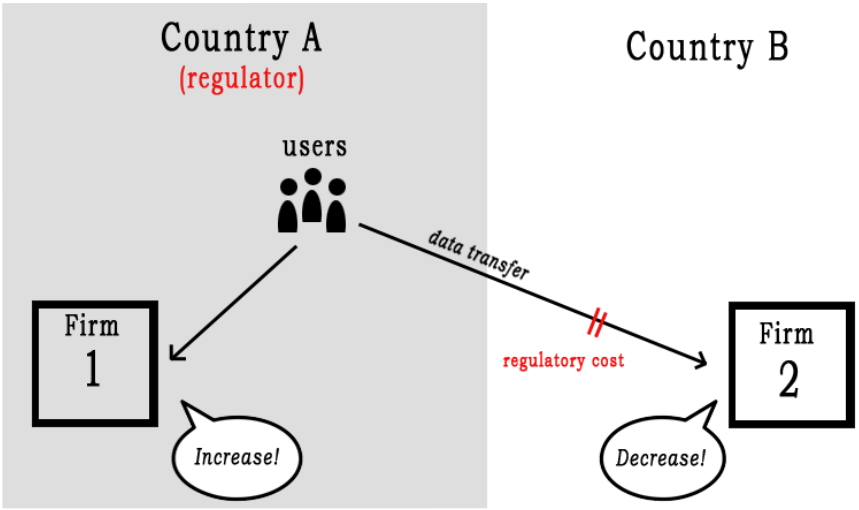
As an example, let's take Firms 1 and 2, both selling their services in Country A. The two firms are identical except for the fact that Firm 1 is headquartered in Country A while Firm 2 is headquartered in Country B.

Let's suppose Country A adopts a law determining that its citizens must provide their consent before their data is used by firms. This provision imposes *homogeneous* adjustment costs to Firms 1 and 2: they both have to ask their users for consent every time they want to use their data.



Now, let's suppose that Country A adopts a law determining that all companies storing its citizens' data outside Country A must adopt special security measures to avoid access from foreign governments. Firm 1 is headquartered in Country A, so it will not suffer any adjustment costs. Firm 2, headquartered in Country B must now pay the cost of these special measures, or buy server space to host data in Country A. Hence, such a provision imposes *heterogeneous* adjustment costs, because it hits a foreign company disproportionately.

[1] Instead, the production of such intangibles have raised. For instance, reproducing a software is almost free, but writing its thousands of code lines is very costly. See De Ridder (2024).



Homogeneous and heterogeneous adjustment costs generate two separate sets of expectations on firms' regulatory preferences. When data regulation adjustment costs are *homogeneous*, both domestic and foreign firms prefer lower adjustment costs (H1). When data regulation adjustment costs are *heterogeneous*, the preferences of domestic and foreign firms diverge. Foreign firms still prefer regulation with lower adjustment costs; instead, domestic firms prefer regulation with *higher* adjustment costs (H2). The reason is that such an increase hits foreign competitors disproportionately, giving the opportunity to domestic firms to increase their market shares or profits.

Adjustment costs	**Domestic business**	**Foreign business**
Homogeneous	Reduce	Reduce
Heterogeneous	*Increase*	Reduce

Table 1: Firms' regulatory preference, depending on the homogeneity of adjustment costs and location.

Of course, many moderating factors play a role. Kennard (2020) identifies a *direct* and *indirect* effect of regulation on firm profits. The direct effect is increasing each firm's production cost. The indirect effect is shifting market share toward low-adjustment-cost firms. In her words, "if firms are relatively close in terms of their adjustment costs, the former will dominate the latter since the shift in market share must be small. As heterogeneity in adjustment cost grows, the impact of regulation on market share grows, eventually overtaking the direct effect of increasing costs". This means that the anticipated adjustment cost difference must be wide and certain enough to generate support from firms. Since the variable costs imposed by regulation are likely proportional to the amount of data that each firm transfers and duplicates, we can predict that the discrepancy in adjustment costs will be higher for firms that are more data-intensive (H3).

4. Quantitative analysis

To test this theory, I employ survey data from an online consultation run in 2021 by the European Commission in the context of its proposal of a regulation called the "Data Act". The Act contained rules on business-to-business, business-to-users and business-to-government data sharing. Among the respondents, I extracted the

answers from firms and business associations (i.e., industry associations and federations of enterprises). The total number of answers by firms and business associations is 192 (79 firms and 113 business associations). Business associations represent dozens to hundreds of firms, and their answers pose the problem of aggregation of preferences: it is very hard to know how the internal discussions between the members of an association determine its final position. I tackled this issue by aggregating and weighting the association members' individual features (see the following paragraphs and the Appendix for further details).

Dedicated literature has shown that EU online consultations may have selection biases since they are voluntary and have a cost in terms of time of completion, despite the online format significantly lowering the barriers to participation (Ferretti & Lener, 2008). However, the problems of representation usually penalise non-business actors like civil society organisations and citizens (Rasmussen & Carroll, 2014). Therefore, I assume that most firms with a significant interest in data regulation had enough resources to answer the consultation, either by themselves or through a representative association.

Dependent variable

To test whether the heterogeneity of adjustment costs plays a role in firms' preferences, I chose a policy proposed in the Data Act that is clearly more burdensome for non-EU companies. The European Commission was worried that foreign jurisdictions might request data from European companies, and proposed three obligations for *any* firms processing European data outside the EU: (i) to communicate to the Commission all foreign laws to which they are subject that might lead to data requests; (ii) to notify their business partners every time they receive a request for access to their data from foreign authorities; (iii) to put in place specified legal, technical and organisational measures to prevent the transfer or access of such data.[2]

By targeting the storage of any EU-originated data in extra-EU servers, such proposals disproportionately impact companies headquartered outside the EU. Even if a company possesses data centres in the EU, data has to be constantly transferred to data analysts who are usually placed in the country where the company is headquartered. Hence, the adjustment costs of these proposals are *heterogeneous* between EU and non-EU firms.

My dependent variable reflects how much these policies are supported by firms. The three options have an increasing cost: communicating legislation updates to the Commission can be considered as a few-times fixed cost; notifying data access requests to business users requires continuous monitoring and is proportional to the quantity of data managed and jurisdictions through which such data flows; finally, putting in place dedicated measures is the most burdensome requirement, because it implies implementing from scratch technical, organisational or administrative procedures. Since these measures are not alternatives and more than one option could be chosen in the survey, I code the dependent variable as the sum of measures supported by each firm: 0.166 for the Commission notification regime, 0.33 for the business notification regime, and 0.5 for the

[2] The Appendix contains the full text of the survey questions.

"dedicated measures". [3] For example, if a firm does not support any measure, its value is 0. If a firm supports *all* measures, its value is 1. If a firm supports the notification to business users and the "additional measures", its score is 0.5 + 0.166 = 0.66. The left part of Figure 1 shows the distribution of the variable across the dataset. More than half of firms and business associations do not support any data regulation, while the remaining ones support various combinations of the proposed policies.

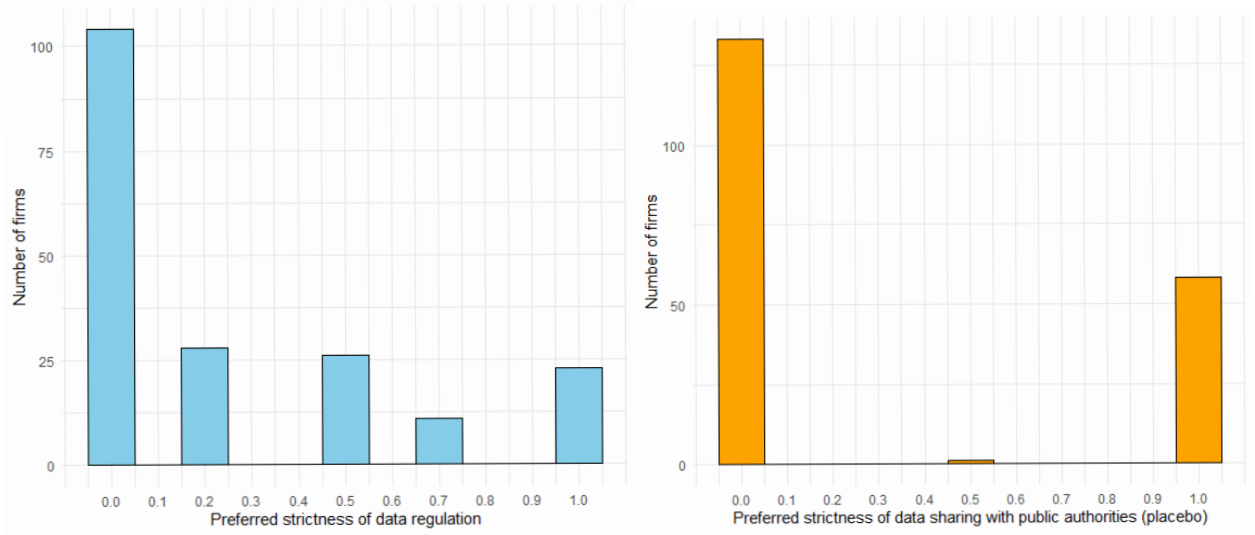


Figure 1: Distribution of the dependent variables (main hypothesis and placebo) across firms.

Independent variables

According to my theory, heterogeneity in preferences is driven by the heterogeneity of regulatory adjustment costs, which in this case are determined by the territory where a firm is storing or analysing data. Hence, the firms' location is the main independent variable. Companies are classified as headquartered (1) or not (0) within the EU territory according to their main legal establishment at the global level.[4] The business associations' score is calculated by averaging the value of their members (0-1) weighted by their size. The assumption is that bigger firms have more power to determine decisions within the associations (Macher & Mayo, 2015; Weymouth, 2012), because contribution fees to join business associations are usually proportional to the size of the firm, and bigger firms have more knowledge and economic resources to promote their interests.

I introduce a series of covariates to check for alternative explanations. First, support for data regulation might be a function of how much a business is reliant on vulnerable data. The survey asked how much the extraterritorial access to data is a risk to the company. I code the variable "data vulnerability" on the basis of the answers: "a minor risk" = 0.33, "a risk" = 0.66, "a big risk" = 1, no risk/answer = 0.

[3] In the Appendix, I test alternative specifications of the dependent variable, for instance by considering only the most expensive measure supported or assuming that the policies have an equal adjustement cost. Also in these specifications, the final results remain significant.

[4] The UK and the non-EU European Economic Area countries (Iceland, Liechtenstein, and Norway) are not considered as part of the European Union.

Size may be an explanatory variable. Given that regulatory costs contain a fixed-cost part, firms under a certain threshold of size or sales might always judge regulation as undesirable. Frey & Presidente (2024) have shown how the GDPR disproportionately harmed Small and Medium Enterprises, and Gulotty's (2020) theory of regulatory protectionism claims that larger, more productive firms benefit from fixed-cost regulations because they force smaller competitors out of the market. On the other hand, smaller firms trade less with foreign companies, so they should be less impacted by regulation on cross-border data flows, and might welcome raised cost of entry for foreign competitors (Weymouth, 2023, pg. 44). Business associations' size is calculated as the average size of their members.

Finally, I use industry fixed effects to control whether firms' policy preferences are determined by belonging to a specific industrial sector. This checks the possibility that specific, data-intensive, sectors suffer disproportionate adjustment costs (as shown by Atikcan and Chalmers 2019). For this purpose, I use the sector classification employed by the EU survey. For business associations, their sector is the one they self-selected in the survey. "Generalist" business associations (i.e., chambers of commerce) are placed in the category "Other".

Placebo test

To further assess the robustness of the results, I conduct a placebo test by applying the model to a policy with *homogenous* costs. The Commission proposed the introduction of rules through which public authorities can access private-sector data when there is a public interest purpose. We can assume that the compliance costs arising from this obligation do not depend on the location of a firm's headquarters. Since the adjustment costs of this provision are *homogenous* across EU and non-EU firms, we should not find any significant relationship with the independent variable. I codify the placebo dependent variable as 1 if the firm/business association answers that a rule of this kind should be introduced by the EU; as 0.5 if it answers "action at Member State level only is needed"; as 0 if it does not think action is needed or does not answer. The right side of Figure 1 shows the distribution of the placebo variable across the dataset.

Results

I test my hypotheses with an ordinary least squares (OLS) regression. My model is specified as follows:

$$RegSupport_j = \alpha_0 + \beta_1 \, \mathrm{EU_j} + \mathrm{X_j}$$

where $\mathrm{RegSupport_j}$ is a continuous variable between 0 and 1, representing how much firm/business association j supports the proposed data protection provisions. My key explanatory variable is whether the firm/business j is headquartered in the EU ($\mathrm{EU_j} = 1$) or not ($\mathrm{EU_j} = 0$). If my hypothesis is correct, the coefficient estimate β_1 should be positive and statistically significant. $\mathrm{X_j}$ refers to a battery of covariates that includes size, data vulnerability and industry-fixed effects.

	Dependent variable:				
	RegSupport				RegSupport (placebo)
	(1)	(2)	(3)	(4)	(5)
EU	0.240***	0.178***	0.177***	−0.009	0.031
	(0.066)	(0.057)	(0.061)	(0.080)	(0.094)
data_vulnerability		0.493***	0.502***	0.041	0.229**
		(0.059)	(0.060)	(0.144)	(0.092)
log(employees)			−0.001	−0.002	−0.011
			(0.007)	(0.007)	(0.011)
EU*data_vulnerability				0.580***	
				(0.166)	
Constant	−0.074	−0.505*	−0.505*	−0.437	0.800*
	(0.339)	(0.292)	(0.296)	(0.287)	(0.455)
Industry Fixed Effects	✓	✓	✓	✓	✓
Observations	192	192	191	191	191
R^2	0.168	0.406	0.415	0.454	0.210
Adjusted R^2	0.087	0.344	0.350	0.390	0.122
Residual Std. Error	0.333 (df = 174)	0.282 (df = 173)	0.281 (df = 171)	0.272 (df = 170)	0.432 (df = 171)
F Statistic	2.067** (df = 17; 174)	6.576*** (df = 18; 173)	6.385*** (df = 19; 171)	7.076*** (df = 20; 170)	2.390*** (df = 19; 171)
Note:					*p<0.1; **p<0.05; ***p<0.01

Table 2: OLS results

The results are shown in Table 2. In models (1-3), location is a significant predictor of whether a firm supports stricter data regulation. This seems to confirm that, when a regulation imposes relatively higher adjustment costs on foreign firms, domestic companies are significantly more likely to support such provisions (H2). Instead, when governments are proposing data provisions with homogenous costs across firms, such as rules to allow public authorities to obtain privately-owned data, business is united across borders (H1): this is demonstrated by the absence of any effect of firm location in the placebo test (model 5).

Companies claiming to be more subject to data access requests are significantly more likely to support data regulation, as shown by the significant effect of the "data vulnerability" variable. This might point to an alternative explanation: it is data management risk, rather than asymmetric adjustment costs, that drives firms' support for enhanced data protection. To investigate this possibility, I explore the interaction between data vulnerability and firm location. If data vulnerability is the main driver of regulatory preferences, we should see that such vulnerability is driving the preferences of firms both inside and outside the EU. Instead, the interaction shows that, among firms with highly vulnerable data, it is only firms that are located in the EU that strongly support regulation. The interaction effect is visible in Figure 1. The more a firm manages risky data, the more the effect diverges: EU companies support stricter regulation, whereas non-EU companies more radically oppose it. From the perspective of a non-EU company, managing more data means more regulatory

costs and, therefore, less support for regulation. From the perspective of an EU company, managing more data means more regulatory costs for *foreign* firms (i.e. because they transfer data to them, for instance, an EU-based company storing data in an Amazon-provided cloud). The more data-intensive the firms, the higher the adjustment costs discrepancy between EU and non-EU companies is. The more, as a consequence, regulatory preferences diverge (H3).

Non-EU firms managing fewer risky data are less anti-regulation because their variable regulatory costs are lower; EU firms managing fewer risky data are more puzzling to explain. Since these firms are managing less data, they might be less aware of the regulatory costs they can inflict on foreign firms.

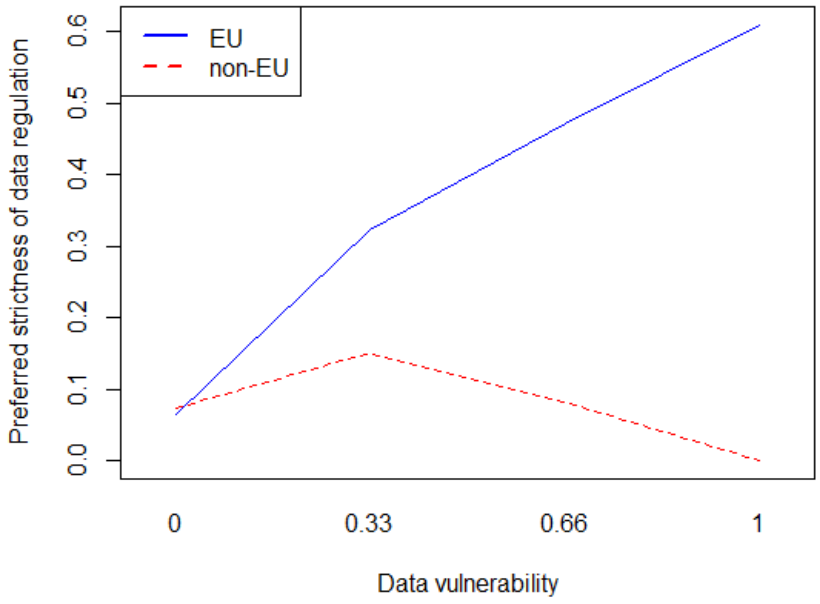


Figure 2: Interaction between firms' location and data vulnerability. The "EU" group includes firms headquartered in the EU and business associations whose EU weighted average score is higher than 0.66. The "non-EU" group includes firms headquartered outside the EU and business associations whose EU weighted average score is lower than 0.33.

5. In-depth case: the sovereignty requirement and the EUCS scheme

The previous sections have shown how firms support stricter data flow regulation when such rules create relatively higher adjustment costs for foreign firms. In this section, I illustrate a specific case showing this mechanism in action.

The "European Cybersecurity Certification Scheme for Cloud Services" (EUCS) is a certification regime that has been drafted by ENISA (European Union Agency for Cybersecurity) since 2019 with the purpose of "enhancing the level of security of a wide range of cloud services" and harmonise security standards inside the European internal market (ENISA, 2020). Although this scheme is voluntary, certain entities might be legally required to adopt it (i.e. public administrations, and firms executing procurement contracts). Between 2022

and 2024, the discussion focused on whether EUCS should include, for the highest level of security ("High+"), a "sovereignty requirement", meaning that such a level can be achieved only if data is stored in the territory of the EU (Digital SME Alliance, 2024).

On one side, many European companies started a lobbying and media campaign to maintain the sovereignty requirement. ASD, a business association representing the European Aerospace, Security and Defence, declared to "strongly advocate for the (re)integration of the High+ requirements" (ASD, 2024). A group of European companies, (including French Capgemini, Italian Telecom Italia, Dassault Systemes, and many others) wrote a public joint letter (EUCS High Plus, 2024) declaring that such requirement is "necessary to mitigate the risk of unlawful data access on the basis of foreign laws" (Chee, 2024). CISPE.cloud, a European cloud business association, called for enhanced data protection measures in the EUCS proposal, by asking for "the choice for all customer data to be stored and processed exclusively in EEA, with options for support located in the EEA" (Schmutz, 2022).

On the other side, strong opposition was advanced by a number of business associations representing non-EU companies, such as the American Chamber of Commerce to the European Union, the Computer & Communications Industry Association (CCIA Europe) and the Information Technology Industry Council (ITI). In a joint position paper, they stated that "The proposed [digital sovereignty] requirements… will create significant entry barriers for non-EU headquartered companies and EU companies with international or global operations". The Japan Association of New Economy wrote that "[i]t could create a de facto market access barrier, hurting both EU and Japanese companies" (Chee, 2023).

The High+ sovereignty requirement is a data protection regulation with heterogeneous costs. When ENISA proposed to scrap such a rule, regulatory preferences split following the line dividing who suffered the lower compliance cost (EU-based businesses) and who suffered the highest ones (non-EU-based businesses). Also, firms promoting "intangible protectionism" in this instance regularly opposed other data regulations with non-heterogeneous costs. For instance, in 2023 ASD opposed the application of NIS2, a new EU cybersecurity Directive that would have increased security-related compliance costs, to its members belonging to the aviation industry (Rullier-Francaud, 2023)., A few months after expressing support for the EUCS sovereignty requirement (Schmutz, 2022), CISPE.cloud recommended the European Commission to "not… introduc[e] ill-conceived additional financial or administrative burdens on Cloud providers" (CISPE, 2023).

6. Conclusion

Why do some firms support data protection regulation despite its economic costs? I argue that they do it to gain an advantage over foreign competitors, by showing that firms holding an advantage in adjustment costs express a stronger preference towards data protection measures with heterogeneous costs. These arguments have important implications for the political economy of digital trade regulation.

The first implication is that pressure for data protection can arise endogenously as a result of competitive dynamics between firms. This points to the fact that, in some cases, the goals of governments, consumers and companies may align on data restriction measures (see also Beaumier & Newman, 2024), potentially shaping "baptists and bootleggers" coalitions of governments, domestic firms and consumer associations (Desombre, 1995). Also, the fact that measures fragmenting global digital trade can be supported by self-interested firms shows a potential self-undermining mechanism of the liberal international order (Farrell & Newman, 2021). This is especially true if companies decide to focus on the domestic market instead of seeking expansion abroad (Liu, 2021).

Secondly, intangible protectionism impacts the distribution of valuable assets in the economy, thus affecting economic growth. A growing literature in economics shows that the rise of intangible assets increases inequality among firms (Haskel & Westlake, 2018) and ultimately harms economic growth by reducing overall innovation since cutting costs by using data acts as an alternative to productivity-enhancing innovation (De Ridder, 2024). This paper shows that companies are strategically aware of the value of data and act to foreclose it, even supporting the reduction of cross-border data flows.

Theorising the political cleavages dividing firms is crucial to understanding how political struggles will shape the institutions that ultimately determine the distribution of data assets among firms – and its economic effects. As advanced by Ding (2024), the way technological leaps are diffused throughout society – and companies – is a crucial factor in economic development and great power competition.

Bibliography

ASD. (2024). *Note on EU Cybersecurity Certification Scheme for Cloud Services*. https://www.asd-europe.org/news-media/publications/asd-position-papers/asd-note-on-eu-cybersecurity-certification-scheme-for-cloud-services/

Atikcan, E. Ö., & Chalmers, A. W. (2019). Choosing lobbying sides: The General Data Protection Regulation of the European Union. *Journal of Public Policy*, *39*(4), 543–564. https://doi.org/10.1017/S0143814X18000223

Baldwin, R. E. (2016). *The great convergence: Information technology and the new globalization*. The Belknap press of Harvard university press.

Beaumier, G., & Newman, A. (2024). When Serving the Public Interest Generates Private Gains: Private Actor Governance and Two-Sided Digital Markets. *Perspectives on Politics*, 1–18. https://doi.org/10.1017/S1537592724001099

Beaumier, G., Newman, A., & Qin, R. (n.d.). *The Politics of Information in an Age of Economic Coercion*.

Chee, F. Y. (2023, December 5). Japanese tech lobby warns against EU cybersecurity labelling scheme. *Reuters*. https://www.reuters.com/technology/cybersecurity/japanese-tech-lobby-warns-against-eu-cybersecurity-labelling-scheme-2023-12-05/

Chee, F. Y. (2024, April 10). Exclusive: Deutsche Telekom, Airbus slam plan allowing Big Tech access to EU cloud data. *Reuters*. https://www.reuters.com/technology/deutsche-telekom-airbus-slam-plan-allowing-big-tech-access-eu-cloud-data-2024-04-10/

CISPE. (2023). *Three steps the European Commission can take right now to help achieving the EU's digital targets by 2030*. https://cispe.cloud/three-steps-the-european-commission-can-take-right-now-to-help-achieving-the-eus-digital-targets-by-2030/

Crasnic, L., Kalyanpur, N., & Newman, A. (2017). Networked liabilities: Transnational authority in a world of transnational business. *European Journal of International Relations*, *23*(4), 906–929. https://doi.org/10.1177/1354066116679245

Culpepper, P. D., & Thelen, K. (2020). Are We All Amazon Primed? Consumers and the Politics of Platform Power. *Comparative Political Studies*, *53*(2), 288–318. https://doi.org/10.1177/0010414019852687

De Ridder, M. (2024). Market Power and Innovation in the Intangible Economy. *American Economic Review*, *114*(1), 199–251. https://doi.org/10.1257/aer.20201079

Desombre, E. R. (1995). Baptists and Bootleggers for the Environment: The Origins of United States Unilateral Sanctions. *The Journal of Environment & Development*, *4*(1), 53–75. https://doi.org/10.1177/107049659500400104

Digital SME Alliance. (2024, September). *EU Certification Scheme for Cloud Services: An opportunity for Europe's Digital Sovereignty*. https://www.digitalsme.eu/digital/uploads/Policy-Paper-EU-Certification-Scheme-for-Cloud-Services.pdf

Ding, J. (2024). *Technology and the rise of great powers: How diffusion shapes economic competition*. Princeton University Press.

ENISA. (2020). *EUCS – CLOUD SERVICES scheme*.

EUCS High Plus. (2024). *Joint Letter—Urgent Call to Action: Inclusion of High+ Criteria in EUCS*. https://eucshighplus.eu/

Farrell, H., & Newman, A. L. (2021). The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining. *International Organization*, *75*(2), 333–358. https://doi.org/10.1017/S0020818320000302

Ferracane, M. F., Lee-Makiyama, H., & van der Marel, E. (2018). *Digital Trade Restrictiveness Index*.

Ferretti, M. P., & Lener, M. (2008). Lay public or experts? E-Participation in authorization for GMO products in the European Union. *Review of Policy Research*, *25*(6), 507–525.

Frey, C. B., & Presidente, G. (2024). Privacy regulation and firm performance: Estimating the GDPR effect globally. *Economic Inquiry*, *62*(3), 1074–1089. https://doi.org/10.1111/ecin.13213

Greenleaf, G. (2021). *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance* (SSRN Scholarly Paper 3836348). https://doi.org/10.2139/ssrn.3836348

Gulotty, R. (2020). *Narrowing the Channel The Politics of Regulatory Protection in International Trade*. University of Chicago Press.

Haskel, J., & Westlake, S. (2018). *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton University Press.

iSPIRTs. (2017). *Response to the White Paper on Data Protection Framework for India*.

Kennard, A. (2020). The Enemy of My Enemy: When Firms Support Climate Change Regulation. *International Organization*, *74*(2), 187–221. https://doi.org/10.1017/S0020818320000107

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. The MIT Press.

Liu, L. (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*, *56*(1), 45–67. https://doi.org/10.1007/s12116-021-09319-8

Macher, J. T., & Mayo, J. W. (2015). Influencing public policymaking: Firm-, industry-, and country-level determinants. *Strategic Management Journal*, *36*(13), 2021–2038. https://doi.org/10.1002/smj.2326

OECD. (2020). *OECD Digital Economy Outlook 2020*. Organisation for Economic Co-operation and Development. https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2020_bb167041-en

Rasmussen, A., & Carroll, B. J. (2014). Determinants of Upper-Class Dominance in the Heavenly Chorus: Lessons from European Union Online Consultations. *British Journal of Political Science*, *44*(2), 445–459. https://doi.org/10.1017/S0007123412000750

Rullier-Francaud, V. (2023). *Applicability of NIS2 to aviation manufacturing imposes an unnecessary burden and is redundant to existing aviation regulations*.

Schmutz, A. (2022). *CISPE Digital Sovereignty Principles*.

Wallach, L. (2025, March 17). The 'Digital Trade' Trap. *Compact*. https://www.compactmag.com/article/the-digital-trade-trap/

Weymouth, S. (2012). Firm lobbying and influence in developing countries: A multilevel approach. *Business and Politics*, *14*(4), 1–26. https://doi.org/10.1515/bap-2012-0030

Weymouth, S. (2023). *Digital Globalization: Politics, Policy, and a Governance Paradox* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781108974158

Appendix

1. **Survey questions**

Dependent variable: *In your opinion, what would be the best solution at an EU regulatory level to mitigate the risk for European companies stemming from the request for access by foreign jurisdiction authorities to their data?*

- Introducing an obligation for data processing service providers to notify to the Commission, for publication on a dedicated EU Transparency Portal, all extraterritorial foreign laws to which they are subject and which enable access to the data they store or process on behalf of their business users (+0.25)
- Introducing an obligation for data processing service providers (e.g. cloud service providers) to notify the business user every time they receive a request for access to their data from foreign jurisdiction authorities, to the extent possible under the foreign law in question (+0.25)
- Introducing an obligation for data processing service providers to put in place specified legal, technical and organisational measures to prevent the transfer to or access of foreign authorities to the data they store or process on behalf of their business users, where such transfer or access would be in conflict with EU or national laws or applicable international agreements on exchange of data
- Providing for compatible rules at international level for such requests. (+0.5)
- I do not know/no opinion (0)
- NA (0)

Control variable: *How likely do you think it is that a cloud computing service or other data processing service provider that is processing data on your company's behalf may be subject to an order or request based on foreign legislation for the mandatory transfers of your company data?*

- This is a big risk for our company (1)
- This is a risk for our company (0.66)
- This is a minor risk for our company (0.33)
- I don't know/no opinion (0)
- NA (0)

Placebo: *Should the EU take additional action so that public sector bodies can access and re-use private sector data, when this data is needed for them to carry out their tasks in the public interest purpose?*

- EU level action is needed (1)
- Action at Member State level only is needed (0.5)
- No action is needed (0)
- I don't know / no opinion (0)
- NA (0)

2. **Aggregation of members' characteristics to code business associations' variables**

When available list of business association's members, and number of members < 1000 (n = 95):

- size = members' average;
- EU score = average of members' location (EU = 1; non-EU = 0) weighted by the size of the members.

When no available list of business association's members available list of members, or member list containing > 1000 firms (n = 18):

- size = average calculated on representative sample of country's firm population, based on the World Bank Enterprise Surveys;
- EU score = deducted from business association's basic information (i.e., Polish Chamber of Commerce assumed as representing mainly Polish firms, therefore EU = 1).

3. **Alternative operationalisation of dependent variable**

Alternative specifications of the RegSupport variable:

- RegSupport_Alt1: each policy is considered as equally costly. Variable is the sum of:
    - Commission notification regime = +0.33
    - business notification regime = +0.33
    - "dedicated measures" = +0.33.
- RegSupport_Alt2: only consider the most expensive measure proposed.
    - No policy = 0
    - Only notification regime (Commission/business notification) = 0.5
    - "dedicated measures" = 1.

	Dependent variable:			
	RegSupport_Alt1		RegSupport_Alt2	
	(1)	(2)	(3)	(4)
EU	0.177*	−0.021	0.143**	0.014
	(0.095)	(0.126)	(0.062)	(0.082)
risk_score	0.712***	0.220	0.484***	0.162
	(0.093)	(0.228)	(0.061)	(0.149)
log(employees + 1)	−0.003	−0.003	−0.004	−0.004
	(0.011)	(0.011)	(0.007)	(0.007)
EU:risk_score		0.618**		0.405**
		(0.262)		(0.171)
Constant	−0.375	−0.302	−0.107	−0.059
	(0.458)	(0.453)	(0.300)	(0.297)
Industry Fixed Effects	✓	✓	✓	✓
Observations	191	191	191	191
R^2	0.359	0.380	0.375	0.395
Adjusted R^2	0.288	0.307	0.306	0.324
Residual Std. Error	0.435 (df = 171)	0.429 (df = 170)	0.285 (df = 171)	0.281 (df = 170)
F Statistic	5.050*** (df = 19; 171)	5.206*** (df = 20; 170)	5.400*** (df = 19; 171)	5.548*** (df = 20; 170)

Note: *p<0.1; **p<0.05; ***p<0.01