UNIVERSITY OF TARTU
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

Ronan McQuillan

The Europeanisation of Third-State Data Protection Regimes: Safeguarding Cross-Border Transfers in Australia and Canada

MA thesis

Supervisor: Dr. Piret Ehin, PhD
Co-supervisor: Dr. Aleksei Kelli, PhD
Tartu 2020

I have written this Master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.
Ronan McQuillan (Signature of author)

The defence will take place on ..... / date / at ..... /
time / ..... / address / in auditorium number ..... / number /
Opponent ..... / name / (..... / academic
degree /), ... / position /

I, Ronan McQuillan
(personal identification code: 39509130064)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation and making thesis public, including for adding to the DSpace digital archives until the expiry of the term of copyright, my thesis entitled; '*The Europeanisation of Third-State Data Protection Regimes: Safeguarding Cross-Border Transfers in Australia and Canada*', supervised by Dr. Piret Ehin PhD & Dr. Aleksei Kelli PhD.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in pp. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.
Done at Tartu on 18/05/2020
Ronan McQuillan
(signature)

Contents

1. Introduction

The question of how and when personal data should be processed is one of the most important emerging issues of our times. In the context of international relations, this has implications for both international trade, and the effective protection of individuals' rights under increasing economic globalisation. The problems therein are twofold. States are more economically dependent on international trade than at any other point in history, while at the same time the increasing digitalisation of most national economies means that the question of how to protect individual data subjects' rights is more pertinent than ever. For these two concerns to be effectively balanced, a great degree of international harmonisation and convergence would be necessary. This is especially true, given the fact that over 70% of states have some form of data protection legislation, either in force or in draft form (UNCTAD 2020). However, this proliferation of legislation carries with it certain challenges, especially given that different states and their respective administrations draft legislation with different priorities and preferences. This problem is exacerbated by the continued failure of certain multilateral organisations to act in this field, most notably the World Trade Organisation, which would in some ways be the expected forum for effective harmonisation of data protection, as a matter inherently linked to the free flows of international trade (Aaronson & Leblond 2018). As such, in the context of divergent national regimes, the question arises as to whether and how a global regulatory regime may emerge in the field of data protection.

The central question of this thesis is whether and to what extent the European Union is emerging as the source of a de facto global regulatory regime for the protection of personal data. Here, a de facto global regulatory regime may be thought of as emerging where separate markets come to the same regulatory choices, without formal cooperation or coordination occurring as such (Lazer 2001). Within the the existing theoretical framework of Europeanisation, this thesis will seek to ascertain to what extent a uniform international policy response is emanating from the EU in the field of data protection. This will make several vital contributions to both the Europeanisation literature, and to the understanding of data protection as an issue within the study of regulatory governance more broadly. Within the field of regulatory governance, data protection is fairly novel, in the sense that it is a highly transnational policy issue, but little international coordination is occurring at the present moment. In the absence of this, it is vital to examine whether or not policy convergence still occurs. Additionally, while some empirical effort has been made to apply the Europeanisation framework to data protection as a policy field, this has borne out relatively mixed

results. To date, where this has occurred it has mainly taken the form of within-case analysis, and so this thesis will also make the contribution of utilising a positivist cross-case methodology to create a more robust understanding of the specific conditions under which Europeanisation of data protection occurs, where previous scholarship has been limited by it's focus on the extent to which Europeanisation has occurred in individual cases.

The rationale behind presuming the EU as a source from which a global regime on data protection is multiple fold. Firstly, in recent years, the most successful harmonisation of different states' data protection regulations has occurred within regional organisations, including the EU, Association of South East Asian Nations (ASEAN), and the Economic Community of West African States (ECOWAS). Of these, the EU is obviously the most likely source of indirect policy harmonisation, on the basis of it being the largest market, as well as having the most stringent regulatory regime in the field of data protection. Additionally, of these international organisations the EU has the strongest base of existing scholarship with regards to exporting its data protection policies, as will be discussed at length in the third chapter of this thesis. However, empirical attention is necessary to ascertain whether and to what extent this is occurring with regards to the present EU regime. Specifically, this thesis will be concerned with determining if any significant degree of Europeanisation can be observed in the data protection regime of third states. The greater the degree of policy transfer from the EU to states outside of its direct regulatory sphere, the stronger the evidence will be that the EU rules are giving rise to a de facto global regulatory regime.

Additionally, there is a well populated body of literature concerning regulatory change emanating from the EU, known as Europeanisation. Where a variety of strands exist within the Europeanisation literature, this thesis will primarily be concerned with two overlapping processes for exporting regulations to wealthy third states, known as *externalisation* and *the Brussels effect*. Both of these processes are well established theoretically, and have previously been applied to a range of policy areas, including data protection. However, their empirical application is generally used to describe events after the fact, while their predictive power remains somewhat unclear, diminishing their overall theoretical value and applicability. In light of this, this thesis will also seek to investigate whether or not regulatory change has occurred according to the theoretical expectations in cases where the theory pre-supposes that it will, in contrast to previous empirical work which has identified regulatory change before seeking to understand whether or not it fits the theory. In other words, a more exact objective of this thesis is to determine to what extent the theoretical expectations described by the Europeanisation literature have been fulfilled with regards to the field of data protection, in order to assess their predictive power. This will make a necessary

contribution to the Europeanisation literature, as, as will be seen, externalisation and the Brussels effect generally apply to states which do not have a particular formal political relationship with the EU, whereas the dynamics of Europeanisation in states which are more closely geographically or institutionally related to the EU has been much more successfully explored already.

The empirical portion of this thesis will specifically comprise an analysis of regulatory changes in Australia and Canada, since the completion of the EU's General Data Protection Regulation (GDPR), with respect to the issue of safeguarding requirements for cross-border transfers of personal data from each of these jurisdictions, as well as the extraterritorial reach of each regime. It is necessary to examine cases outside of the EU's formal regulatory jurisdiction which are themselves both wealthy markets with highly developed regulatory capacity, in order to ascertain that regulatory convergence is occurring independently of direct or formal coordination. There are multiple reasons for choosing to focus solely on the issue of cross-border data transfers for systematic analysis. Firstly, it is necessary to adopt a narrow focus, as analysing the entirety of the regulatory regime in each case is an endeavour well beyond the scope of this thesis. In light of this, the issue of cross-border transfers is most appropriate given that, as will be discussed at length later, this is an area where to present EU regime is particularly innovative and novel, and the influence of the EU would therefore be more easily observable in third states. Additionally, cross-border transfers are the facet of any data protection regime which is most pertinent to international relations scholarship, in the sense that they are the most directly related to issues of international trade, and the inter-state politics contained therein.

The remainder of this thesis will precede according to the following structure of chapters. Firstly, the theoretical framework of Europeanisation will be laid out, beginning with its general principles and core tenets, followed by how these function in the more specific context of exporting regulatory regimes to highly economically developed third states. Secondly, there will be a discussion on the history and background of data protection as a policy issue, including the varying historical approaches employed by states and other international actors, with a specific focus on how this has been approached by scholars of international relations to date. Thirdly, the exact methodological framework for measuring the Europeanisation will be laid out in detail. The fourth chapter will comprise the empirical portion of this thesis. This will first involve analysis of each of the cases to ascertain the extent of Europeanisation in each, followed by a discussion and comparison of theses findings. The thesis will end with concluding remarks on the implications of this, and the potential for further research thereafter.

2. Europeanisation of Third States

This chapter will be concerned with providing an overview of Europeanisation, as the theoretical grounding of this thesis. Specifically, it will first explore the central arguments of the Europeanisation framework, and some of the different applications of these to date. It will then outline the specific strand of the Europeanisation literature of concern to this thesis, specifically how regulatory policies and practices are theorised to be exported to wealthy third states through processes known as *externalisation* and *the Brussels effect*. This will be accompanied by a discussion of the mixed empirical success of these processes to date. Specifically, it will be presented that these have generally only been successfully applied post-hoc to events in individual cases, while their predictive power remains unclear, including in the context of cross-case comparison. This will comprise a discussion of both their theoretical difficulties, as well as where they have been empirically argued to have occurred or not to have occurred. The goal of this is to give a theoretical grounding to this thesis' goal of assessing whether or not these process have any real world predictive power, including in the context of data protection, by providing an exposition of how these processes are theorised to work.

2. 1. The Europeanisation Framework

One broad definition characterises Europeanisation as the diffusion of European ideas and practices across time and space, typically with specific regards to the EU (Flockhart 2010). The notion of, 'ideas and practices' contains a broad range of artefacts and phenomena, including concrete governance instruments like legislation, policies and institutions (Börzel & Risse 2011), as well as more normative factors, like norms, values, identities and behaviours (Jacquot & Woll 2003). In practice, this provides a fairly large degree of flexibility, both in terms of conceptualisation and research agendas within the Europeanisation literature. Within this broad range of possibilities, a narrower definition which is more suitable to the aims of this research is the process by which policy areas in a certain state become increasingly subject to EU policy making (Börzel 1999: 574). However, even within this narrower definition, there remains room for conceptual flexibility, in the sense that the outcomes of Europeanisation may still vary from changes in individuals' behaviour to institutional adaption, while the exact triggers of Europeanisation may equally vary between direct requirements places upon states by the EU and the adoption of new domestic practices and preferences from increased contact with the EU or

European states, either by individuals, governments or institutions (Lodge 2002). The triggers are generally referred to as adaptational pressures.

Additionally, the various objects of Europeanisation also correspond to different logics through which Europeanisation can occur. The first of these is the logic of *rational choice*, wherein actors in a target state are provided with material incentives by the EU to create certain changes in their domestic polity. Here, Europeanisation occurs when these incentives outweigh the costs of doing so, either materially or politically (Mastenbroek & Kaeding 2006: 333). The other major logic underlying Europeanisation is that of *constructivism*, wherein normative impetuses for domestic change exist, including alterations of the identities, norms and values of domestic actors in response to increased social contact with the EU (Flockhart 2010). To a certain extent, a tension exists between these two underlying logics of Europeanisation, at least in as far as the fact that individual authors have their own ontological preferences and points of view. However, the two theoretical positions are not necessarily mutually exclusive. For example, there is little to suggest that Europeanisation of normative factors like identities would not ultimately facilitate rational choice Europeanisation, and so it is perfectly reasonable to assume that the processes may occur in tandem Rather the fact that both have received considerable successful empirical attention indicates that it is prudent to consider both the rational choice explanations for certain instances of Europeanisation, as well as their normative underpinnings. Nonetheless, with such variation existing within the concept of Europeanisation, it is worth considering the different contexts in which the term has been deployed to properly understand its usage.

Early scholars of Europeanisation were mainly concerned with emerging structures of governance at an EU level, with a view to analysing both the impact of these on member states, and the member states' own role in shaping them, respectively referred to as top-down and bottom-up Europeanisation (Risse, Cowles & Caporaso 2001; Börzel 2002). In other words, this strand of Europeanisation concerns the emergence of the EU as a new institutional centre among the member states (Buller & Gamble 2002). A key element of this is domestic actors within member states *uploading* their policy preferences and practices to the EU level (James 2007), and therefore shaping the character of governance at an EU level. However, a certain degree of competition occurs between member states seeking to upload their preferences and practices, with each seeking to minimise the costs of adapting their own domestic ways of doing things when an EU-level standard eventually emerges (Knill 2001). In this sense, it is clear that the member states impact on the EU level and vice versa can hardly be separated, in the Europeanisation by either of these modes is essentially triggered by the need to unify policy practices within the boarders of the EU to

achieve fundamental goals of European integration, such as the completion and continued functioning of the Single Market, or the effective guaranteeing of citizens' rights across the Union. As such, strand of Europeanisation scholarship is essentially concerned with how and why European integration occurs.

Shortly thereafter, focus shifted to include the impact of EU ideas and practices outside of the EU's territory. This was spurred in part by the changing international environment after the end of the Cold War, which was accompanied by what has been described as a move by the EU from the politics of *exclusion,* to the politics of *inclusion* (Smith 1996). This led to the EU seeking greater influence in the post-bipolar order, primarily by attempting to mould states in its immediate neighbourhood in its own image, a process which has been referred to as the external projection of internal solutions (Lavenex 2004). The most prominent example of this is changes being required in accession candidates, or potential candidates, with the adoption of EU norms and practices being used as a direct and conscious condition of accession, in a process known as *conditionality* (Schimmelfennig & Sedelmeier 2004). This is exemplified by successive rounds of Eastern Enlargement from 2004 onwards. However, this type of conditionality is not limited to the accession process. Indeed, it occurs anytime the EU sets conditions on external states, in exchange for meeting some material reward, which may also include association agreements, market access, aid, or access to visas, among others (Schimmelfennig 2010). In any case, the desire for this touted reward among either governments or individuals within a state forms the adaptational pressure for Europeanisation to occur.

However, one of the major areas of contestation within the Europeanisation literature relates to why these adaptational pressures are effective. Central to this are different conceptions of the EU's power as an actor within the international system. Europeanisation via conditionality is linked to the C*ivilian Power Europe* thesis, which holds that the the EU is a novel actor in its usage of non-military means to achieve its extraterritorial goals (Orbie 2006). In practice, the tools available to the EU to do so effectively in the context of conditionality are its market power, and regulatory capacity and expertise, as can be seen in the enlargement process, as well as other spheres where conditionality is employed, such as the Eastern Neighbourhood Policy or recent bilateral deals with Turkey to handle the migration crisis (Gregou 2019). However, as a broadly realist account of conditionality's effectiveness, this conception of the EU's power is somewhat incomplete on its own. This fact gives way to the *Normative Power Europe* thesis, which holds that the the EU's power in the international order primarily comes from its ability to shape ideational factors in other countries, including norms, values and identities, as well as perceptions of what constitutes

appropriate behaviour (Manners 2002). Both the normative and civilian power theses have been derided for being indeterminate and vague, in the sense that debates surrounding their respective validity and explanatory power relative to one another seem unproductive (Schimmelfennig 2010). However, this endeavour to characterise the EU as an exclusively normative or civilian power ignore the fact that the EU undoubtedly acts as both in how it influences other states. As we have seen how the civilian component of the EU's power operates through Europeanisation via conditionality, it is worth turning attention to how Europeanisation may occur as a result of normative triggers.

Often, this involves attention being paid to the transfer of ideas and practices to citizens and individuals, as opposed to states and governments. One of the key ways this occurs is with regards to the issue of national identities in EU member states, as well as other countries in the European region (Spohn & Triandafyllidou 2003). Other normative factors which are externally projected through Europeanisation often relate to the core values of the EU itself, including rule of law, democratic norms and human rights (Gergana & Aydin-Düzgit 2012; van Hüllen 2011). In these instances, the adaptational pressures for states to apply these norms come from pressure from their citizens. This may be expressed through electoral politics, lobbying, or simply through these ideas diffusing through the society in question. In extreme cases pressure may also be put upon governments through public demonstrations, for instance the 2015 EuroMaidan Protests in Ukraine (Onuch 2015). This mode of Europeanisation is referred to as *socialisation*. Where conditionality alters the cost-benefit calculations of domestic actors in a state, socialisation brings about change by altering their perceptions of what is appropriate behaviour, often as a result of wanting to be or appear properly 'European' (Schimmelfennig 2010). However, none of this is to say that the processes are necessarily entirely separate. Indeed, the two generally occur simultaneously. The crux of this is that socialisation can equally take effect within domestic institutions and arms of the state, and the institutional logic within these is then altered. In light of this, a greater degree of socialisation may make domestic governments more amenable to conditionality, making it difficult to distinguish between the two processes entirely.

Additionally, Schimmelfennig identifies *imitation* as a mode of Europeanisation which is closely related to socialisation. The distinction between the two is that socialisation occurs as a result of conscious efforts by the EU to shape actors' conceptions of appropriate behaviour, where imitation occurs simply because the EU is a visible and successful model from which to emulate solutions to domestic problems (Schimmelfennig 2010: 328). The adaptational pressure here is the low costs of adoption incurred by simply emulating existing solutions to a domestic problem, rather

than creating these from scratch. A number of conditions facilitate Europeanisation through imitation. Firstly, states in a position of uncertainty are more likely to look towards role models to imitate, and when this occurs they are likely to choose to imitate the EU if they find that its modes of governance resonate with their existing beliefs and preferences (*ibid.*). Second, the presence of transnational networks of policy professionals, civil servants, NGOs, commentators and other actors is necessary to facilitate this emulation by allowing learning to take place (Trondal 2005). Schimmelfennig presents uncertainty in this context as being a 'novice in the international system', and therefore requiring a model to emulate, presumably as a result of low levels of expertise or institutional capacity and experience. This functions irrespective of territoriality. However, it is difficult to see why this could not also apply to specific policy areas, as opposed to how a state should conduct itself in the international system more generally. Specific policy areas where Europeanisation by imitation has been borne out include renewable energy regulations and sustainable development goals (Busch & Jörgens 2011; Laffery & Jörgens 2004). In this sense, uncertainty appears to extend to new, emerging, or fast moving policy areas, where emulation is therefore a cheaper, easier and more expeditious means of solving domestic governance problems. Additionally, imitation has been observed among other regional organisations' governance structures (Schimmelfennig 2010: 336), lending more weight to the idea that the novelty of a policy issue facilitates imitation.

A constellation of different forms of Europeanisation can therefore be seen to apply to states with different relationships with the EU, ranging from member states, to accession candidates, dependent neighbours and finally to distant states with no particular relationship with the EU. Despite this, there are multiple factors which are common to each of these forms of Europeanisation. At the most basic level, each tries to explain whether, to what extent and why policy convergence emanates from the EU (Nicholaides 2010). Of course the most basic precondition of this is the presence of some EU level policy or practice to be projected. This leaves a question mark over how successful Europeanisation should assessed or measured. One approach is to measure institutional change in the target country as a dependent variable (Börzel & Risse 2012). However, this is somewhat problematic as convergence through Europeanisation has been demonstrated in terms of policy outcomes or approaches to certain policy issues without uniform mimicking of institutions necessarily occurring (Perkins & Neumayer 2004). While institutional change is no doubt highly indicative of Europeanisation, exclusive focus on this fails to account for the fact that target states may substantially converge with EU policies and practices without necessarily using the same institutional structures or legislative instruments to achieve this end.

Indeed, to the extent that it is possible, states experiencing Europeanisation are likely to incorporate EU policies and practices into their existing systems and structures of governance, as this lowers the costs of adoption by eliminating the need for excess institutional change. To better understand this, it is necessary to consider a principle at the heart of the Europeanisation literature - the *goodness of fit* hypothesis.

2. 2. Goodness of Fit

All kinds of Europeanisation are dependent on the *goodness of fit* between the target polity and the EU in the specific field or policy area in question. That is, the existing compatibility between European policies, norms and institutions, and their domestic equivalents in the target state (James 2007). This is most important in the context of Europeanisation to external polities, as internally, states are ultimately required to conform to EU standards, irrespective of their domestic policies or the costs of changing these. With regards to third states, a certain degree of *misfit* creates pressure in the target state to adapt to European practices. However, where too much misfit exists, adaptational pressure is outweighed by outsized costs of adoption. By contrast, where there is insufficient misfit, there is also insufficient adoptions pressure, even though the opportunity costs are low. As such, Europeanisation only generally occurs where a moderate goodness of fit exists (*Ibid.*). For example, in the context of conditionality, the adaptational pressures may comprise the desire to gain access to the Single Market, along with other political incentives contained within an association agreement. By contrast, the costs of adoption in this example include those incurred in meeting requirements under the *acquit communautaire*, as well as setting up new institutions. Additionally, costs for certain domestic actors would come along with adopting core values of the EU. For instance, greater emphasis on rule of law, democratic norms and good governance would create problems for those individuals or institutions within a state which engage in corruption. Europeanisation will not occur unless the adaptational pressures created by a moderate goodness of fit outweighs these costs.

While the right balance of adaptational pressure and costs are preconditions for Europeanisation, this must also be facilitated by certain other domestic factors. Börzel and Risse (2002) identify two concurrent processes whereby adaptational pressure can lead to concrete domestic change, one in a rationalist vein, and the other more normative. The first is that coalitions of actors with shared interest in creating domestic change are able to achieve this where there are few *veto points* and generally *facilitative institutions* (Börzel & Risse 2002: 7). By contrast, diverging interests among major domestic actors creates veto points, inhibiting Europeanisation.

Similarly, non-facilitative institutions, or high concentrations of formal power can prevent adaptational pressure from translating into actual changes in policy. For example, in regulatory matters, certain national administrations which are averse to stringent regulations, along with coalitions of non-export orientated companies who would not benefit from the regulatory regime becoming Europeanised may act as veto points. The second is that domestic actors act as *norm entrepreneurs*, promoting European ways of doing things. This is facilitated by cooperative informal institutions, to the point that, over time, new norms are incorporated into the domestic political culture, leading to domestic change (*Ibid.* 8). This may include the normative basis of specific regulations. In other words, this would involve recognition of the need to regulate from a certain normative point of view, for instance consumer rights or environmental concerns, such that European standards are met. The main obstacles to this are competing norm entrepreneurs.

However, the goodness of fit hypothesis has born out relatively mixed empirical results, leading scholars of a diverse range of policy fields to seek out intervening explanatory variables (Falkner *et al.* 2005: 89; Knill & Lenschow 1998: 610). This has led to the causal link between misfit and adaptation being described as spurious, and that it should therefore be disregarded, with focus then being placed on the policy preferences and beliefs of domestic actors concerning the EU policy at hand (Mastenbroek & Kaeding 2006: 338). However, this argument is made exclusively in the context of Europeanisation of EU member states, and seems to hold little weight when considering extraterritorial Europeanisation. This is because third-state domestic actors preferences and beliefs concerning EU policies cannot be disentangled from the impact these policies will have on them. That is, in this context they can only have preferences and beliefs about whether or not adoption is worthwhile in terms of the costs incurred. In this sense, while it is undoubtedly fruitful to take account of domestic actors' policy preferences, misfit continues to be the impetus for policy transfer. As such, a more complete and rigorous approach is to take account of both of these things. Rather than discrediting the goodness of fit hypothesis, mixed empirical results highlight the need for further scholarship to elucidate how this theoretical expectation occurs in the complex real world of the international system.

2. 3. Externalisation and the Brussels Effect

Compared to the various modes of Europeanisation which have been discussed already, less empirical has been paid to the Europeanisation of wealthy and industrialised third states outside of the EU's immediate neighbourhood. In some ways, this is unsurprising, as this kind of Europeanisation is more challenging to observe. The crux of this is that, where Europeanisation

within the EU and its immediate neighbourhood is generally a direct and deliberate process, the same cannot be said of wealthy third states (Schimmelfennig 2010: 328). Instead, what Schimmelfennig classifies as *Europeanisation to OECD countries*, occurs by an indirect process known as *externalisation,* where the EU does not seek to export its standards, but rather they are mimicked by interdependent markets and polities due to the size and importance of the Single Market (*ibid.* 334). It should be noted however, that non-membership of the OECD would not preclude externalisation, nor does OECD membership in itself have much to do with externalisation, but rather this is used as a short-hand for countries which are similarly economically developed to the EU. Successful externalisation occurs when there is a high level of trade interdependence with the EU, and where the EU regulations are particularly strong and centralised in the policy field at hand (*ibid.*). Within this framework, the strength and centrality of EU regulations are a function of the division of competences within the EU for a given policy area. In this sense, while Europeanisation through externalisation is a distinct process from internal Europeanisation, the two are not entirely separable.

Similarly, externalisation is a separate process from other methods of EU external governance, but a certain overlap nonetheless remains with these. The EU's other major market-based tool of external governance is *conditionality*[1], where certain policy positions are required of third states as a condition of their trading relationship with the EU, through a deliberate process of international negotiations (Smith 1998). However, this is most commonly utilised against smaller or less wealthy jurisdictions, or those seeking to eventually gain EU membership, among other political goals (Grabbe 1999; McKenzie & Meissner 2016; Linan Norgueres & Hinojasa Martinez 2001), as in negotiations with larger or more powerful states, the EU has less leverage and so more traditional inter-state bargaining occurs. Additionally, conditionality is more often utilised for the purpose of exporting more normative policies, like human rights, or else to achieve more general EU foreign policy goals, rather than as a tool of regulatory governance (Schimmelfennig 2010: 328). However, this does not preclude conditionality being used in negotiations with large or interdependent states in specific policy areas where the EU has considerable leverage. Nor is it impossible for externalisation and conditionality to occur simultaneously. Obviously though, this leads to different outcomes than where externalisation alone occurs, as the outcome of any international negation is dependent of the relative bargaining power of each actor (Kremenyuk 1988), and so the extent of policy transfer is inhibited by the EU being forced to make concessions.

[1] While conditionality can also make use of political incentives, for example association agreements or visa access, access to the Single Market naturally remains one of the most effective incentives available to the EU.

Here, one of the key real-world difficulties of the theoretical expectations of externalisation can be seen, in that it assumes that the target state is above a certain threshold of economic power, but remains unwilling or unable to exert its own regulatory preferences, at least in a given policy areas. This makes externalisation's predictive power somewhat dubious, in the sense that it is highly caveated and contingent on a very unlikely situation.

Of course, even in terms of theory, this still leaves a question mark over how exactly externalisation occurs. For one thing, if the size of the Single Market and the strength of specific EU regulations alone were enough to ensure externalisation, then there is little in Schimmelfennig's explanation to suggest that the same extent of regulatory influence wouldn't be observed coming from other large markets[2]. In other words, we must consider what it is that is apparently unique about the EU in this respect. This requires familiarity with what has come to be known as the *Brussels Effect,* which describes the process by which other wealthy jurisdictions indirectly adopt EU standards, where Schimmelfennig's externalisation merely describes the outcome. Bradford (2015) effectively breaks this into two stages. First, a *de facto* Brussels Effect occurs, where individual export-orientated companies in a third state adopt EU standards internally, to retain their ability to operate in the Single Market. Then a *de jure* Brussels Effect may occur when these companies lobby their national governments to adopt EU standards, so that they must only follow a single set of rules, as well as giving them a competitive advantage over their domestic competition with lesser capacity to follow stringent regulations (Bradford 2015: 159). As such, the initial impetus for a Brussels Effect is the significance of the EU export market to domestic companies. The theory suggests that the EU is uniquely able to export its standards in this way, due to a combination of its market size, regulatory capacity, preference for high regulatory standards in consumer matters, and the non-divisibility of these standards (Bradford 2020: 25). However, the Brussels Effect is only able to occur where foreign companies are unable to move their operations in part or as a whole to escape high regulatory standards, and can be limited by companies pursuing alternative markets with lower standards, or where another jurisdiction exports standards which are as restrictive as those of the EU (Sinopoli & Purnhagen 2016: 99).

It is also worth considering how the goodness of fit hypothesis functions in the context of Europeanisation via externalisation and the Brussels Effect. In this specific instance, it follows that adaptational pressure stems from the need to gain or retain access to the EU market. Since

---

2. The most commonly cited instance of another jurisdiction having the same regulatory impact is the US state of California's influence in the field of environmental standards, where a California Effect has been observed to play a similar role (Vogel 2009: 6). The two terms are often used interchangeably, without regard for the source of regulation, especially in older literature.

externalisation generally occurs with regards to regulatory matters, costs of adoption mainly comprise changes to the existing regulatory regime, including the drafting of new policies and institutional change for governments, as well as private actors adjusting to these new rules and ways of doing things. Goodness of fit can also comprise the general regulatory culture and disposition within national polities. Private companies may also see the need to comply with a stricter regulatory regime as a cost in and of itself, and will as such only be willing to do so where the cost of losing EU market access outweighs this. Additionally, costs of adoption may occur as a result of regulatory competition, where other large markets export standards which conflict with those of the EU, or where there exists a better goodness of fit between these and the existing regulatory regime in a target state. This would create a situation where a certain degree of trade may have to be sacrificed with this third market in order for Europeanisation to occur via the Brussels Effect. Alternatively, a Brussels Effect may be prevented by veto players which have an interest in maintaining the status quo or advocating a different regulatory regime entirely.

Empirical scholarship has to some extent borne out the theoretical expectations of the Brussels Effect, but it has also revealed a number of intervening factors which can prevent or limit its success. For instance, a *de facto* Brussels Effect has been observed in certain wine-making firms in New Zealand, but a *de jure* effect could not materialise because other large markets, including Japan and China had equally restrictive regulations in this field, and there was not sufficient overlap between all of these for a common, overarching regulation to encompass the requirements of each (Klüche 2017). This gives a strong indication that the EU is not in fact in a unique position to export its regulatory preferences, as the theory suggests. Princen (2003) observed a limited Brussels Effect in the regulation US and Canadian fur trapping, in the sense that some, but not all, elements of the EU regulation in question were externalised. Here, he concludes that the combined market size of the USA and Canada, along with the threat that whey would be successful in a dispute-resolution process against the EU at the World Trade Organisation served as an impetus for the European Commission to enter bilateral negotiations, which eventually hindered the success of the Brussels Effect (Princen 2003: 151). However, studies into the Europeanisation of ICT and telecommunications sectors in third states have demonstrated a whole-sale success of the Brussels Effect, giving rise to possibility that individual regulatory areas may provide more fruitful ground for this kind of Europeanisation (Cantero Gamito 2018). What this demonstrates is that externalisation via the Brussels Effect is a complex and multi-actored process where myriad obstacles and veto-players can emerge. This, in turn, potentially hinders the theoretical predictive

power of this type of Europeanisation, and highlights the need for ongoing empirical scholarship in order to understand the exact conditions under which a Brussels Effect occurs.

2. 4. Externalisation and the Brussels Effect as Regulatory Governance

Of course, externalisation and the Brussels Effect can hardly be separated from the broader literature on *regulatory governance.* Helpfully, certain knowledge of this concept is elucidating when considering the obstacles to Europeanisation via these processes. Regulatory governance can be thought of as the making, monitoring and enforcement of rules and norms, by a diverse range of actors, including national governments, international organisations, independent agencies, businesses, civil society and even individuals (Levi-Faur 2010). Here, rules and norms can comprise hard-governance through legislation and public policy, as well as soft-governance like codes of conduct, professional standards, certification schemes and appropriate behaviours. Taken in sum, these actors and their outputs form a *regulatory regime* within a given polity (Drezner 2008). This is crucial, as it means that the formation of a regulatory regime is a diffuse process, with competing interests among the various actors involved. Conflict of interests between different actors within a polity is known as *vertical regulatory competition* (Trachtman 1993: 53). For example, even within the smallest national regulatory regime, businesses and civil society are likely to have irreconcilable regulatory preferences. Since externalisation and the Brussels Effect can essentially be thought of as the subsumption of third states into the European regulatory regime in particular policy fields, it is little wonder that actors within the third state with conflicting interests can become obstacles and veto players to this, and that as such a Brussels effect may be easy to observe ad-hoc, without certain conditions guaranteeing that one will predictably occur.

While this is already a fraught process when individual states are considered in isolation, the problem becomes multitudes worse within the international environment. This is because, at this level, *horizontal regulatory competition* can emerge, where actors at the same level in different polities compete for regulatory and market power on the international stage (Trachtman 1993: 51). In most instances, this involves inter-state regulatory competition. In one school of thought, this creates a *race-to-the-bottom*, where one state may lower its regulatory standards to become more attractive to inward investment, only to be mimicked by others in an effort to retain their competitiveness in the international market (Radaelli 2004). Here, internationally operating companies can relocate their operations to the jurisdiction with the lowest regulatory standards, and therefore the lowest costs of operating. Expanding this logic to the topic at hand, it then stands that, where two similarly sized export markets with different regulatory dispositions are available to

companies in a given state, then these companies should be more inclined to do business with the market with lower regulatory standards, due to increased efficiency and lower costs of adoption. A full Brussels Effect, therefore would not be expected take place, as this is effectively the opposite of race-to-the-bottom regulatory competition, where the highest standards prevail in the international regulatory regime.

This however, presupposes that corporations are actually able to escape higher levels of regulation by relocating their operations, which is often not the case, particularly with regards to regulations emanating from the EU. Whether or not a corporation is able to move operations to escape a restrictive regulatory regime is related to the *elasticity* or *inelasticity* of the target of regulation itself (Bradford 2015). An elastic target provides scope for doing this, by primarily regulating issues surrounding a business' operations, like employee protections or corporation tax. Here, corporations are able to move to certain operations other jurisdictions to avoid these, while still retaining access to markets where these regulations exist. By contrast, the EU primarily creates inelastic regulatory targets, creating consumer protections relating to the final product or service that the company offers (*ibid.*). Corporations are therefore unable to avoid the costs of adopting these regulations without forgoing access to the Single Market. For example, a manufacturer of consumer goods would be able to avoid environmental regulations relating to their manufacturing process by moving their factories outside of the EU, but they would be unable to do so to escape similar regulations on the performance of their actual end products. In the context of the Europeanisation, this goes a long way towards explaining why certain regulatory areas have a greater chance of seeing a successful Brussels Effect occur. As will be seen, the current EU regulatory regime in the field of data protection is particularly inelastic, given its focus on protecting all EU citizens, irrespective of where their data is processed or stored, and is therefore, in theory, almost the ideal policy area for a Brussels effect to occur, and as such also an ideal policy area to test its predictive power.

From the preceding discussion of the externalisation via the Brussels Effect, and the characteristics of the EU data protection regime with regards to the safeguarding cross-border data transfers, the hypothesis emerges that *the more significant the EU market is to the national economy of a third state, the more Europeanisation will occur.* The following chapter will provide a background on the phenomenon of data protection, as it it has been approached as an issue of regulatory governance in the international relations and broader political science literatures to date.

3. Background on Approaches to International Data Transfers and the GDPR

In the 21st century, the issue of data protection straddles a number of core areas of interest to the study of international relations. The goal of this chapter is to provide a sufficient overview of this topic for a political science readership. This will involve a discussion of how and why this is of interest, including in terms of the dynamics of power in international trade, the role of states in controlling and regulating trade, and differing international priorities with regards to the protection of rights of individual citizens and populations. This will also involve a discussion of how the issue of personal data protection has been approached by scholars of international relations to date, across each of these areas of concern. Additionally, this chapter will provide a basis for understanding the key issues and principles which make up different approaches to how data is protected in the context of international data transfers, both historically and in terms of recent innovative legal instruments, specifically the EU's General Data Protection Regulation (GDPR). This chapter will conclude by discussing the core approach to international data transfers adopted by the EU, with a view to outlining how Europeanisation may be theorised in this context.

3. 1. Background

To understand the the current picture of how data usage is regulated around the world, we must first survey historical approaches to this issue, first at a state level and, later, internationally. While some international regulatory harmonisation exists, disparity continues internationally with regards to the question of how and what data should be collected, stored and processed, including a notable transatlantic rift (Peltz-Steel 2015). This is even apparent in the different terminology used by policy makers in the United States and Europe. As a result of fledgling new information technologies, debates around the use and potential misuse of personal data first arose in the US in the early 1960s. The primary concern here was that the storage and use of data by government bodies for unknown reasons constituted a threat to the privacy of individual citizens, as enshrined in the US Constitution (Westin 1970: 312). To date regulation of data usage in the US is framed in terms of *privacy*, which Westin defines in this context as '*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'* (*ibid*. 7). The US Federal regulatory regime only applies to state bodies, aside from a small number of industry-specific pieces of legislation in sensitive fields such as healthcare and security (Tan 1999; González Fuster 2014).

By contrast, *data protection* is a European coinage, which retains a great degree of overlap with *privacy*, but is nevertheless conceptually and practically distinct. Once again, to understand the contemporary European approach to data protection, it is first necessary to explore its historical contingencies. The term *data protection* entered English from the German *Datenshutz* after the German State of Hesse passed the *Hessische Datenschutsgesetz*, the world's first piece of data protection legislation, in 1970, and thereafter became the preferred terminology across the continent (González Fuster & Gutwirth 2013). While still limited in scope to information collected and processed by public bodies, this act nonetheless pioneered certain features which today characterise the modern European data protection regime, as will be outlined more fully later in this chapter. Most notably, it is the first instance of an independent data protection authority being established (Bennett 1992: 77). It quickly became a fruitful basis for the drafting of national legislation in European countries throughout the 1970s, including Germany, France and Sweden. While these differed in norms, scope and aims, they variously contained elements which would later defuse and become codified throughout the EU, including applicability to both public and private actors; recognition of the need for data protection beyond the goal of *privacy;* the prohibition of data collection and processing with the subject's consent; separate protections for 'sensitive data'; and the right of individuals to access and rectify any data held on them (González Fuster 2014: 70). In the same period, Austria became the first country to establish the right to data protection as a constitutional guarantee (*ibid.* 67). However, as these regulatory innovations occurred, so too did disparities between them create a need for alignment and harmonisation.

3. 2. Early International Regulation of Data Protection

In the late 1970s, two international organisations made concurrent efforts to harmonise the data protection regimes of their members. Specifically, the Organisation for Economic Cooperation and Development (OECD) and the Council of Europe (CoE) sought to standardise data protection and privacy laws, to avoid economic and social progress being inhibited by regulatory divergence (Kirby 2011: 8; de Terwangne 2013). First, the OECD adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). In the process of drafting these, we can already see the dynamics of regulatory competition occurring. In a process of international bargaining The American position that other countries' higher regulatory standards should not impede cross-border data flows was seen by the Europeans as an attempt to create a US hegemony in this area of trade, while the European preference for eliminating trade restrictions in balance with the protection of individuals by creating uniformly high standards was seen by US negotiators as a

kind of non-tariff based protectionism (Bennett & Raab 2003: 74). The Guidelines were successful in establishing eight common data protection principles across OECD members; *Collection Limitation; Data Quality; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability* (OECD 1980). While these remain influential, they are vaguely worded, with no fixed standards under any of the principles, and they are not in themselves legally binding, although OECD members commit to their implementation. However, member states must also endeavour not to enact policies which would create obstacles to international data flows by adopting standards which are higher than the minimum requirements set out in the Guidelines (*Ibid.*). As such, in this early instance of harmonisation, we can clearly see how US interests prevailed in direct international negotiations, resulting in harmonisation by a race to the bottom.

By contrast, the CoE, as an organisation explicitly concerned with promoting human rights in Europe, was far less concerned with eliminating trade barriers than harmonising human rights standards. It's *Convention 108 for the Protection of Individuals with Regards to the Automatic Processing of Personal Data* (1981) sought to guarantee the same level of protection for individuals across the territories of all signatories in terms of data protection, including but not limited to the right to privacy (CoE 1981: art. 1). Through this human rights lens, Convention 108 was highly influential on what would eventually become the 'European' approach to data protection (González Fuster 2014: 93). Pioneering elements of Convention 108, as the first international instrument explicitly concerned with data protection as opposed to privacy, include the standardisation of the definition of 'data' across ratifying countries as information regarding an '*identified or identifiable individual'* (*Co*E 1981: art. 2), as well as containing the first international recognition of the need for additional protections for sensitive categories of data, including those relating to ethnicity, religion or political beliefs (*ibid.* art. 6). In terms of the actual protections contained within, we can also see the influence of Convention 108 on the contemporary EU data protection regime, as will be apparent later in this chapter, including stipulations that data should *be collected and processed fairly and legally; stored for specific and legitimate purposes; adequate, relevant and not excessive to these purposes; not kept for longer than is required for these purposes; accurate and up-to-date; accessible, amenable and erasable by the subject* (*ibid.* art. 5, art. 7, art. 8.). Convention 108 is also innovative in stipulating that, where these protections have not been met, subjects must have effective remedy in front of national courts (*ibid.* art. 10).

However, despite its innovation and influence, Convention 108's failings and limitations also provided fruitful ground for action by the then European Economic Communities (EC) in the field of data protection. Notably, the Convention offers an ambivalent stance on data transfers to

non-party states, neither requiring nor preventing these (Greenleaf 2012: 83). Instead, Article 12 prohibits restrictions on data flows between parties, except where the other party doesn't provide sufficient protection for a certain category of data, or where the other party is used as an intermediary to transfer data to a non-party (CoE 1981: art. 12.2&3). Whether or not a party allows transfers to a non-party is outside of the scope of Convention 108, and therefore a matter of national law in each of the signatories (Bennett & Raab 2003: 73). Rather than setting a common standard among parties to Convention 108 for transfers to non-signatories, this creates a rather impractical scenario where each party must establish that each of the others provides an adequate level of protection relative to its own, in order to have confidence that transfers to these will not result in its national law being circumvented. Additionally, Convention 108 failed to uniformly guarantee remedies for data subjects across parties, where infractions occur, as well as being definitionally somewhat vague on certain key terms (Greenlead 2012: 84; Fromhol 2000: 467). As will be seen in the following section, this represented insufficient coordination on the issues of cross-border data transfers and effective guarantees of citizens' rights for the EC to meet its goals in creating the Single Market, without creating its own legislation.

3. 3. European Union Data Protection

Throughout the 1970s, the Parliament of the EEC sought to pressure the Commission to legislate for data protection within the community, but the latter chose not to do so until the completion of Convention 108 and the OECD guidelines, on the basis that these may prove sufficient (González Fuster 2014: 120). Indeed, when Convention 108 was completed, the Commission published a recommendation that all EEC member ratify this, on the basis that it was an appropriate instrument for creating a 'uniform level of data protection in Europe', in terms of both protecting the rights of individual and eliminating barriers to trade within the Community (81/679/EEC: I.2-5). However, in practice, this quickly proved to be untrue, especially given the shortcomings of Convention 108 outlined in the previous section. Inconsistent implementation of Convention 108 across EEC members quickly exposed the need for Community level legislation in this sphere, as member states with higher levels of protection began restricting data transfers from members with comparatively weak protections, most notably the case of the French data protection authorities barring transfers between the Italian and French subsidiaries of the Fiat corporation (Meunier & McNamara 2007: 113). In this sense, the need for EEC level action in this policy sphere was instigated by the emergence of high standards within individual member states problematising

the goal of completing the Single Market, and as such should be considered an instance of bottom-up Europeanisation.

This eventually led the, by then, European Communities (EC) to adopt the *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (95/46/EC). By then the EC had also developed its Three Pillar structure, wherein the Directive falls under the first pillar, dealing with economic cooperation and the internal market. To that end, its preamble cites Article 100 of the *Treaty Establishing the European Community,* which gives the Commission competence to legislate for all matters concerning the internal market, as its legal basis (TEC: Art. 100.1). While the innovations of the Directive are too many to innumerate, the most significant to the goal of this thesis and the discussion so far is on the subject of restrictions of data flows to third countries. Specifically, Article 25.1 of the Directive stipulates that data may only be transferred to third countries which provide 'adequate' levels of protection. Member states and the Commission are required to notify one another where a third country's protections may be inadequate, which the Commission will then issue a binding decision on whether or not this is the case (95/46/EC: art. 25.2-6). These decisions involve examining relevant legislation in the destination country and soft-governance instruments like professional codes, as well as the types of data in question and the details of its usage, in light of the other stipulations and principles outlined elsewhere in the Directive. The Commission is then mandated to enter negotiations with third states to raise their standards, such that they become adequate.

This specific development in the Directive is crucial, as it gave way to some of the most important scholarship on the Europeanisation of third states' data protection regimes to date, and to the examination of data protection policies through an international relations lens more broadly. Much of this concerns what is known as the *Safe Harbour* compromise, a scheme under which individual US companies were able to adopt internal data protection policies which were deemed adequate to receive transfers of EU data, without the need for comprehensive federal legislation or the creation of an independent data protection authority, as was the EU's preferred outcome. This compromise emerged after a bilateral negotiation process, in which the preferred US outcome was essentially European recognition of self-regulation by individual corporations and organisations. One strand of the literature, in a constructivist vein, explains the *Safe Harbour* compromise as resulting from dialogue between two interdependent actors which leads to value-change in both, and eventually a compromise which does not resemble the initial preferences of either (Farrell 2003). By contrast, realist scholarship holds that as the US economy was comparatively more dependent on open data flows with the EU than vice versa, a compromise emerged weighted towards the

European preference in a process of conventional interstate bargaining (Busch 2006). This latter explanation appears more convincing when we consider other states' responses to the Directive, including Canada, where, as a smaller trading power than the US, a greater degree of Europeanisation was observed in the late 1990s and early 2000s, including the passage of comprehensive legislation and the establishment of an independent authority (Bennett & Raab 2003: 98; McClennan & Schick 2006). The argument has been made that respective changes in each case represent a successful Brussels Effect to different degrees (Princen 2009). However, this is far from conclusive and renewed scholarship is required, especially since, as will be seen, the GDPR has greatly reduced the prospect of inter-state negotiations relating to international data transfers.

3. 4. The GDPR and Data Transfers to Third States

Data protection was given the status of a fundamental right in the *Charter of Fundamental Rights* (2000), which became legally binding with the passage of *Treaty of Lisbon* (2009). This fact, along with rapid technological development in the 21st century gave the European Commission both the competence and impetus to pass more far reaching data protection legislation beyond the goals of the Single Market, in the form of the GDPR (González Fuster 2014). During its two year implementation period, the UK's Information Commissioner characterised the GDPR as '*an evolution in data protection, not a burdensome revolution'* (ICO UK 2017). In line with this characterisation, its six core principles are not in themselves a far removal from the those of the other legal instruments already discussed. They are *fairness and lawfulness; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality (GDPR art. 5-11).* While it is vital to be aware of these principle for the analysis that will follow, the extent to which higher levels of protection under each has been discussed extensively in the literature (eg. Goddard 2017; Albrecht 2016; Buttarelli 2016; EUFRA 2018), and is, in any case, well beyond the scope and aims of this thesis. In a similar vein, the GDPR's definition of 'data' is not far removed from previous definitions of information surrounding identified or identifiable individuals, but this is expanded to include any factor '*specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'* (GDPR art. 4.1). More novelly, the GDPR is applicable to any actor globally which collects or processes the data of EU residents, regardless of territoriality (GDPR art. 3).

More pertinent to the subject and aims of this thesis is the control and regulation of data transfers to third states, as outlined in in Chapter V of the GDPR. Besides international agreements, this is permissible in two instances, such that the protection offered to data subjects is not

undermined (GDPR rec. 101). The first of these is on the basis of an *Adequacy Decision* by the European Commission (GDPR art. 45). In essence, this is a binding decision which may be made that a certain third state offers equivalent data protection, either generally or sectorally, subject to ongoing monitoring and consultation. Specifically, this takes account of domestic law in the territory of the third state, as well as their existing commitments regarding data protection under international law. However, the Court of Justice has ruled that this does not require an exact replication of EU law, but that the Commission should outline its reasoning that the state in question provides equivalent protection (Eur-Lex: C−362/14). In the instance of such a Decision, data may free slowly from the EU to recognised third states and international organisations, subject to any territorial or sectoral limitations outlined in the specific Decision. While national supervisory authorities in EU members continue to have the competence to hear claims from citizens regarding the transfer of their data to third states, no additional requirements are placed upon the organisation exporting this data.

In the absence of an adequacy decision, data transfers to third countries are generally only permissible where the data controller has put in place appropriate safeguards, such that data subjects retain their enforceable rights and can access effective legal remedies (GDPR art. 46). This can occur in a number of ways, including legally binding agreements between public bodies, as well as private actors implementing approved codes of conduct and certification schemes (GDPR art. 40 & 42). However, the primary data protection safeguards are *standard contractual clauses* and *binding corporate rules* (EUFRA 2018: 258-62). Standard contractual clauses, which have been approved by the European Commission or national supervisory authorities, are legal text which can be inserted into contracts to hold signatories to the principles of data protection contained within the GDPR, ensuring enforcement and effective legal remedies where breaches occur (GDPR art. 46). Where data transfers occur between a group of enterprises or as part of a single economic activity, data transfers are permissible under binding corporate rules (GDPR art. 47). These must be legally binding, and provide effective remedy for infringement of all principles contained within the GDPR. Additionally, they must explicitly state the mechanism for cooperation with data protection authorities, and the processor based in the territory of a member state must accept liability for any infringements of the binding corporate rules. While these are the primary instances when data transfers may occur, derogations also exist where data subjects give explicit consent, where the transfer of a subject's data is required to fulfil a contract they have entered, or in instances of individual or public interest (GDPR art. 49).

4. Research Design

4. 1. Research Design

The empirical portion of this thesis will comprise a small-N cross-case comparison, employing a most similar systems design (MSSD). As Europeanisation of third-state data protection regimes via the Brussels Effect is a theoretically derived expectation, this is an appropriate research design, as it is particularly well suited towards testing theoretical hypotheses in the real world, as well as elucidating the mechanisms of causality (Smith 2010). This works by providing empirical evidence for abstract expectations, and providing context for how these function in reality. Small-N comparisons then facilitate the connection of, often disparate, theories and theoretical expectations to empirical observation (Blatter & Haverland 2012: 144). In this regard, they are powerful knowledge creation tools, as they allow for a better understanding of both the theoretical literature, and concrete phenomena. While small-N research designs are often derided for failing to establish robust theories, this can be disregarded as little more than a matter of epistemological preference. Indeed, the value of small-N research lies not in allowing us to make generalisations about the world around us, but in providing in-depth causal stories by examining a small number of cases, and in doing so improve our knowledge of the topic at hand (Gschwend & Schimmelfennig 2007: 11). However, their ability to do so rests on the correct choice of cases for each research problem.

More specifically, a MSSD research design is appropriate where the independent variable varies from the outset and the values of the dependent variable do not factor into the research design itself, but rather they are then measured to deduce whether or not one causes the other through a process systematic comparison to ascertain whether or not variation occurs in the dependent variable (Anckar 2008). Here, systematic comparison requires that the cases are as similar as possible across all variables, except for the independent variable under examination (*ibid.*) The goal therefore is to approximate control across all variables which have the potential to influence the outcome of the independent variable, to ensure that causality can be established as emanating from the independent variable. Given this, an MSSD research design is the ideal vehicle for empirically testing the predictive power of a theory, in the sense that cases can be selected which vary along the lines of the theoretical requirements in terms of the independent variable, and the dependent variables can then be measured to assess whether or not the theoretical expectations are met, and therefore whether or not the theory provides any real-world predictive power.

4. 2. Case Selection

Specifically, this thesis will examine the cases of the Australian and Canadian data protection regimes, and their responses to the new requirements and protections concerning cross-border data transfers brought in by the GDPR. In any MSSD research, the key to appropriate case selection is finding cases which differ in the independent variable of the study, but are otherwise as similar as possible (Gschwend & Schimmelfennig 2011: 149). This involves controlling any and all variables which may affect the outcome of the dependent variable. For the purposes of this research problem, the logic behind choosing the cases of Canada and Australia is as follows. Firstly, both are parliamentary democracies, with British-derived common law systems. This must be controlled, as it could impact the ability of private actors to lobby legislators, which is crucial for a successful Brussels Effect. Both have similarly developed economies, with the GDP per capita in both falling within the 45,000-55,000 USD range (WorldBank 2020), this is crucial, as it has already been discussed how the wealth of a nation relative to the EU is a key factor in whether or not a Brussels Effect occurs. Additionally, each of their economies are primarily made up of the service sector (OECD 2020), and both cases have adoption rates of digital technologies well above the average, scoring with 0.02 points of each other on the World Banks Digital Adoption Index (WorldBank 2020). Both of these variables must be controlled, as they impact the pertinence of data protection to domestic actors. Finally, the two cases have broadly similar GDPs, with Canada's being around 1.7 trillion USD and Australia 1.4 trillion USD in 2018 (WorldBank 2020), making both similarly highly developed economically.

Additionally, this case selection allows for a degree of grounding in earlier empirical work on the Europeanisation of third-state data protection regimes. Specifically, it has been established that a certain degree of Europeanisation via a Brussels effect occurred in Canada in the wake of the 1995 Data Protection Directive (Bennett & Raab 2003). Similarly, it has been established that Australian privacy reforms in the 1990s were also a direct result of the passage of the EU's Directive (Birnhack 2008). As such, this selection will make it possible to revisit these case to see if the same dynamics of Europeanisation occur with respect to the GDPR in the same way they did with the Directive, particularly in light of the changed role of adequacy decisions, as outlined in the previous chapter. In this sense, studying these two cases will allow this thesis to make one of its core contributions by taking two instances where Europeanisation has previously been shown to have occurred, and carrying out a systematic comparison to better understand the causal mechanism at play, which is taken to be the economic relationship with the EU in terms of trade in services. In this regard, this case selection is well places to contribute to a broader understanding of the

dynamics of converging regimes in international regulatory governance, especially where formal coordination does not occur. The thesis will therefore be fruitful in contributing to a sounder theory of how regulatory convergence occurs in these circumstances.

As a final point on the subject of case selection, it is also crucial to consideration the variation between cases in terms of the independent variable. A certain additional challenge emerges here in the sense that the externalisation and the Brussels Effect take economic interdependence as pre-conditions (Schimmelfennig 2010). Indeed, it is well established that more one-side trade dependence will inhibit Europeanisation via these modes (Dimitrova & Dragneva 2009). While the operationalisation of the independent variable will be discussed momentarily, in terms of case selection it is important to note at this point that the values of this will necessarily fall within a more narrow range, such that both cases can both justifiably be described as economically interdependent with the EU, as opposed to a research design where one case was wholly dependent, or had little economic relationship with the EU to speak of. In light of this, it is necessary to choose two economically interdependent cases, where one has a consistently higher value for the independent variable than the other over time, although the difference year-to-year may be quite small. This is to overcome any issues of validity, which would stem from the fact that little causal inference made from smaller variations in values taken at a single point in time. As can be clearly seen from the figures 1, 2 & 3. which proceed from the following discussion on the operationalisation of the independent variable, Canada has seen a consistently higher value in terms of *the significance of the EU market to export orientated companies* over the past decade. As such, while both can be described as economically interdependent with the EU, Canada's higher value can more convincingly form part of a causal inference, thereby supporting the Brussels Effect's expectation.

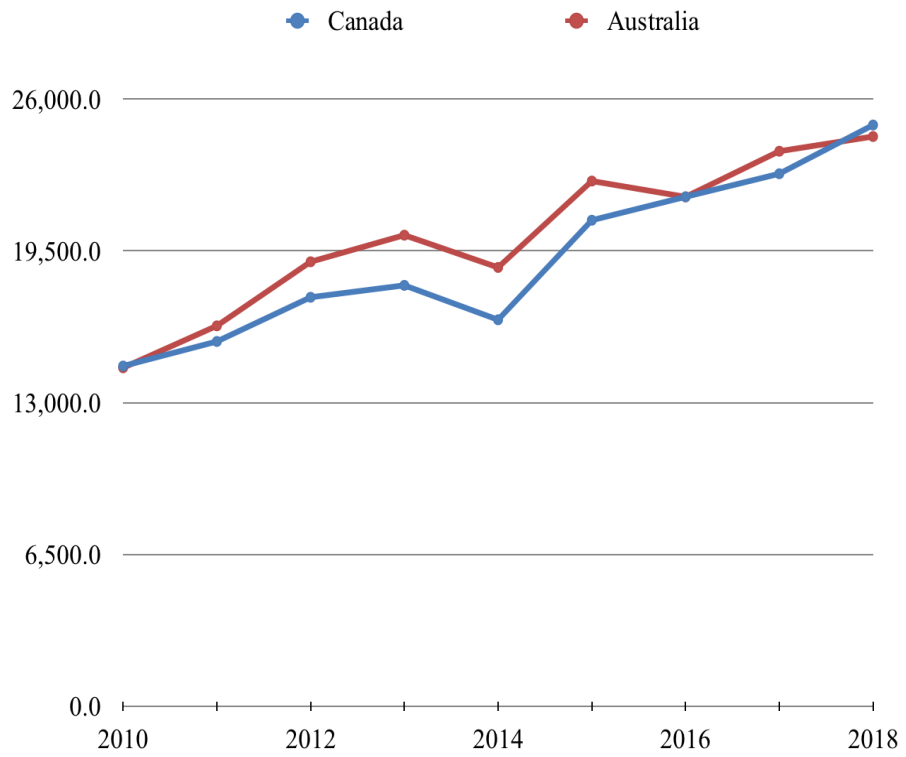
4. 3. Operationalisation

Given the nature of the Brussels Effect, as already discussed, the independent variable in this analysis can be taken as *the significance of the EU market to export-orientated domestic companies* in each of the cases. However, this obviously requires further operationalisation. Specifically, *the deficit in trade in services with the EU* will be taken as a proxy variable for this. A proxy variable measurable variable which stands in for immeasurable or unquantifiable variables (Wickens 1972). In this instance, this will take the form of the difference between imports in services from the EU and exports in services to the EU in each case, where both cases import more services than they export, therefore running a trade deficit. To stand as a proxy for the significance of the EU market to export-orientated companies, the deficit in trade in services with the EU will

have an inverted relationship with the hypothesis. That is, a lower trade deficit indicates that more services are exported to the EU relative to the value of those which are imported, meaning a greater overall significance of the export market to domestic companies. It is crucial to understand that a lower value in the proxy variable here therefore actually corresponds to a higher value in the independent variable, as more Europeanisation would in theory be expected in the case with the lower trade deficit.

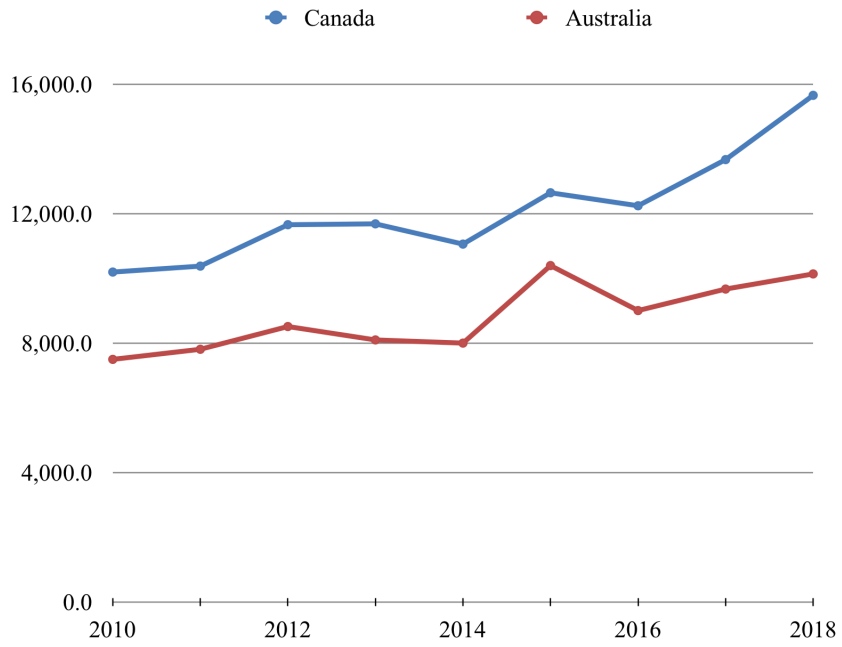
The specific logic behind this choice of proxy variable is two-fold, given that the *significance* of one sector to a national economy is somewhat abstract. Firstly, thebalance of services which are exported and imported to and from the EU in each case is an indicator of both the number of export orientated companies, as well as the relative market power of each case compared to the EU. This in turn influences the combined lobbying power of export orientated companies, and therefore their ability to instigate a full de jure Brussels Effect. Secondly, exports in services have been selected, as this necessitates the collection and processing of personal data of EU citizens to a far greater degree than the export of physical goods. The only exception to this is the export of goods directly to consumers through e-commerce platforms, but this is relatively insignificant in the scheme of overall national GDP, and is in any case not reported separately from other exporting of goods. As such, it is better to disregard the export of physical goods entirely and focus on services, so as not to cloud the picture with data which is irrelevant to the research problem at hand. *Figure 1.* and F*igure 2.* show each case's imports in services from the EU and export in services to the EU respectively.

Figure 1. Canadian and Australian Imports in Services from EU 2010-2018 (€1,000,000)



(EU Commission 2018)

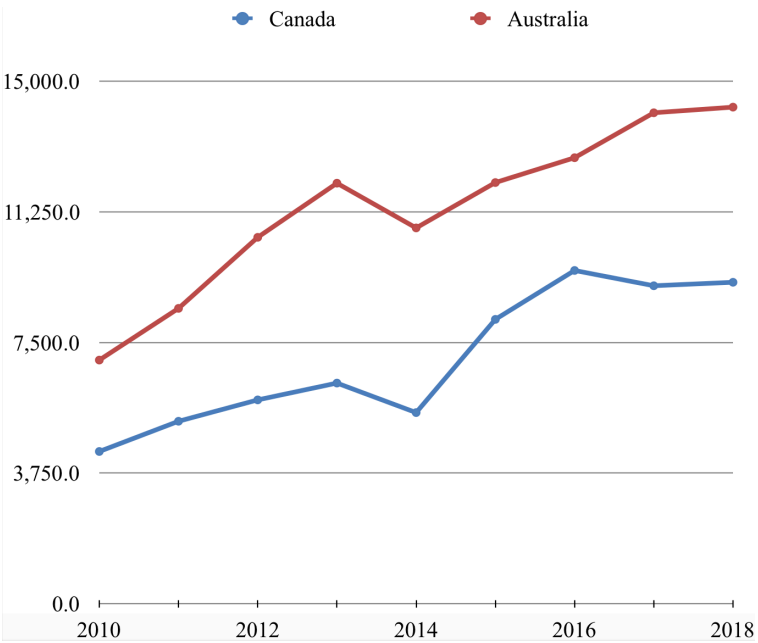
Figure 2. Canadian and Australian Exports in Services to EU 2010-2018 (€1,000,000)



(EU Commission 2018)

As can be seen, the two cases display similar values in terms of imports in services, but differ greatly with regards to their exports. *Figure 3.* shows that Canada has quite consistently seen a lower value in its service-trade deficit than Australia over the last decade, with their respective averages in the period shown being €7,039,500,000 and €11,341,900,000. In this sense, there is a clear and consistent variation between them, within the confines of the necessary trading relationship. As such, a greater degree of Europeanisation is expected in Canada than Australia.

Figure 3. Canadian and Australian Trade-In-Services Deficit with EU 2010-2018 (€1,000,000)



(EU Commission 2018)

Regarding the dependent variable, the extent of Europeanisation of the respective data protection regimes with regards to safeguarding requirements for cross-border transfers, this can essentially be operationalised as the level of similarity and equivalence of each case's instruments to Chapter V of the GDPR, on transfers of personal data to third states and international organisations in terms of the required safeguarding mechanisms. From each of the articles of this chapter, a set of key indicators of Europeanisation can be derived. These are equivalent provisions for *the general principles for external transfers* (art. 44); *transfers on the basis of adequacy decisions* (art. 45); *transfers according to appropriate safeguards* (art. 46); *binding corporate rules* (art. 47); *enforceability of external judicial decisions outside of internal law* (art. 48; rec. 115); *derogations for specific situations* (art. 49); and *international cooperation for the protection of personal data* (art. 50). An additional indicator will comprise the specific instruments and form of governance

used to make these provisions, including whether hard-governance through legislation or soft-governance, like codes of conduct, are utilised. This is appropriate, given the Court of Justice' position in *Schrems V. Data Protection Commissioner* (Eur-Lex: C−362/14), that equivalent protections need not necessarily be *verbatim* copies of the GDPR, or even take the same form to be recognisable to the Commission or national data protection authorities. However, where provisions are linguistically similar and utilise similar instruments of governance in the form of specific legislation, this nonetheless still indicates a higher level of Europeanisation than would otherwise be the case.

However, ascertaining relative levels of Europeanisation from qualitative data poses an additional challenge when comparing the two cases. Thankfully, this can be alleviated by turning to existing taxonomies of Europeanisation. One such taxonomy respectively characterises low, moderate and high Europeanisation as taking the form of *absorption, accommodation,* and *transformation* (Orbie & Carbone 2016: 4). Here *absorption* refers to incorporating certain European elements, without substantially altering domestic structures. *Accommodation* means adapting certain policies, institutions or procedures, without altering their essential character or the logic which underlies them. *Transformation* can be thought of as fundamental change in policies, procedures and institutions, including in terms of their essential character and underlying logic (*ibid.*). The methodological value of adopting such a taxonomy lies in the ability to more easily compare the outcomes of Europeanisation in each case. Obviously, this is most true in an instance where the different cases fall within different categories along this ordinal scale, thereby allowing easy comparison of the extent of Europeanisation in each (Kamden & Swyngedouw 2000). However, this existing taxonomy will additionally be helpful in the instance that both cases fall within the same ordinal category, by providing sufficient criteria to allow within-category comparison. For instance, it is perfectly conceivable that both cases may fall within the accommodation category, but more accommodation may be observable in one case than in the other, in terms of the extent of adaptation of policies, institutions or procedures.

4. 4. Research Methods

In terms of the method of measuring and comparing Europeanisation across cases, the empirical part of this thesis will comprise a fairly straightforward employment of *content analysis*. This is the systematic reviewing and analysis of textual data through a rigorous *analytical code* to elicit empirical knowledge (Bowen 2009). As the goal of this is to establish the level of equivalence in each case to provisions contained in Chapter V of the GDPR, Chapter V itself will form the basis

of the analytical code, with specific reference to each of the key indicators outlined above. The establishment of such a robust code is crucial to ensure the objectivity of content analysis, and therefore the validity of any inferences which can be made regarding the extent of Europeanisation in each case in terms of the safeguarding mechanisms in place for transfers to third states (Krippendorff 1989: 404). Where content analysis is sometimes derided for putting forward subjective interpretations, or allowing researches to project their own biases by making assumptions about the context or intention of the document in question's drafting (Bowen 2009), this is unlikely to pose a particular problem for this specific research, as the former can be elucidated through a degree of exposition of the background in each case, and the latter is fairly self-evident given the regulatory genre of documents in question.

An additional methodological challenge is posed by the ruling in the *Schrems* case that provisions under data protection regimes in third states must not be formally similar to those of the GDPR in order for them to offer equivalent protection. That is to say, it disincentivizes legislatures in third states to mimic the GDPR formally, allowing them to instead use legislative instruments which are more amenable to their existing legal culture, while still experiencing Europeanisation. To overcome this, the logic of the *functional method* from comparative legal studies will be borrowed and employed. This method concerns itself with seeking out functional equivalence, rather than superficial similarities in language or form (Platsas 2008). Again, the instance of such similarities would not be ignored, as they would indicate a greater degree of direct policy transfer than provisions which are only functionally similar. Rather, it is important to emphasise the existence of exclusively functional similarities does not in itself display an absence of Europeanisation, as long as equivalent protections are still provided under the six key indicators outlined above. Any adverse validity effects of the search for functional equivalence can be mitigated by thorough explanation of how such equivalence has been identified throughout the analytical portion of this thesis, such that they are objectively verifiable.

Where necessary, a certain degree of *process tracing* will also be applied through the course of examining the safeguarding mechanisms in place in each case, especially where these have changed. This is not to meet the primary research goal of establishing the extent of Europeanisation across cases. Rather, it is necessary as process tracing is a useful tool for adding inferential leverage, and therefore adding empirical weight to the establishment of causality, especially where the expected causal mechanism is theoretically derived (Collier 2011). This is a common strategy in small-N cross-case comparisons, as this type of research design needs to be supplemented with within case analysis in order to make a more meaningful causal inference (Collier, Brady &

Seawright 2010). In other words, while it would be possible to demonstrate a correlation between high significance of the EU market with Europeanisation in each case, process tracing is additionally necessary to confirm the Brussels Effect as the causal mechanism which underlies this. Additionally, if the hypothesis is the disconfirmed, process tracing in the exposition of each case will be invaluable in identifying the reasons why, including any real world obstacles or veto-players which may have inhibited the Brussels Effect in one or both of the cases. In turn, this would allow this thesis to still make an empirical contribution to the Europeanisation literature, even if it's core hypothesis proves to be untrue, by elucidating some of the limitations of the Brussels Effect.

4. 5. Data and Sources

The collection of appropriate data and sources for the empirical portion of this thesis will be relatively unproblematic. The requisite data for the independent variable has already been displayed above. This is publicly available from the European Commission. Likewise, the necessary data to establish the extent of Europeanisation is freely available to the public, as it relates to public policy. Specifically, these will be Chapter 8 the *Australian Privacy Principles* (APPs) the *Australian Privacy Act* (1988; amended 2019), and the Canadian Privacy Commissioner's Guidelines for Processing Personal Data Across Borders, which accompany the *Personal Information Protection and Electronic Documents Act* (PIPEDA), as well as PIPEDA itself. Where appropriate, relevant caselaw and decisions of the respective data protection authorities will also be referenced, to give a fuller picture of the regulatory regime, as it operates in practice. It will also be necessary to examine the pre-GDPR regulatory regimes in each case, to confirm that they previously had similar levels of goodness of fit. Finally, where relevant, each case will take account of other public documents, like policy papers, including consultations from the data protection authorities.

5. 1. Empirical Analysis: Australia

Case Background

The Australian privacy regime is centred around the *Privacy Act*, which was passed in 1988, to meet Australia's obligations as an OECD member (OAIC). In keeping with this, its applicability only extended to the process of personal data by federal and state agencies. Despite this relatively narrow scope, almost immediately following its entry into force, the Privacy Act began receiving media criticism for being too restrictive, both in preventing public servants from carrying out essential duties, as well as allowing government officials to avoid scrutiny by citing privacy concerns as a justification for withholding information (Campbell 1989; Taylor 1989). However, these concerns eventually largely abated, and in the years following the EU's Data Protection Directive, the Privacy Act received substantive amendments, to extend its applicability to the private sector, as well as creating an independent Information Commissioner's Office (Privacy Act: amend. 2000). It has been argued that this was a direct response to the passage of the Directive, such that EU members would continue to transfer their citizens' data to Australia, subject to adequate protections being offered there (Kohen 2002: 709). While this direct influence of the EU on the Australian data protection regime is somewhat speculative, rather than empirically proven as such, this early instance of regulatory convergence nonetheless appears to indicate the salience of EU regulations to Australian legislators in this field.

Regulatory Regime and Governance of External Transfers

Like the GDPR, external data transfers in Australia are regulated by primary legislation, in the form of Section 5B of the Privacy Act, along with Chapter 8 accompanying Australian Privacy Principles (APP) from the *Office of the Australian Information Commissioner*. However, before considering the provisions contained therein, it is necessary to place these in the context of the preceding chapters of both documents. One crucial element of this is applicability. The Privacy Act and APP make a distinction between APP entities and non-APP entities (Privacy Act: 6.C-F). Non-APP entities, to which the legislation does not apply, include registered political parties, certain government authorities, and businesses which turn over less that $3,000,000 AUS per year and have no corporate link to an APP entity (Privacy Act: 6.D-E). By contrast, the GDPR provides no such general exceptions, instead offering only situational derogations in matters of individual or public interest (GDPR: art. 86-91), as well as the effective delivery of health and social services (GDPR: art. 9.2.h-i). In this sense, the Australian data protection regime can be thought of as generally less

stringent in its applicability, by virtue of offering these general exceptions, including in the context of international transfers. The small business exception was slightly revised in substantive post-GDPR amendments to the APP (OAIC: 2019), however, it's continued existence in its current form could nonetheless be problematic in the context of trade with the EU, as it offers a strong potential for small businesses in Australia to be used to facilitate onward transfers of EU data to other states with even weaker regimes. As such, this is one area where a Brussels Effect would have been particularly expected.

Similarly, the Australian regime differs somewhat in its applicability to external actors. Where the GDPR applies to the processing of data anywhere in the world, where the subject of this data is within the EU (GDPR: art. 3.2), the Privacy Act and APP's external applicability introduces the concept of an *Australian Link*. One element of this is similar to the GDPR approach, in that the regime is applicable to external actors which collect data concerning subjects *in Australia* (Privacy Act: 5B.3C). A linguistic key difference between the applicability of the GDPR and the APP in this regard is their respective focus on *processing* and *collection*. For example, the latter creates a situation where the Privacy Act would not be applicable in an instance where data concerning an Australian resident was collected while they were temporarily in another territory, while the former protects EU residents when ongoing external processing occurred in a similar situation. In this sense, the Australian regime is functionally less effective in its external applicability. This article was already present in the pre-GDPR text of the Privacy Act, and so policy transfer of the higher European standard cannot be said to have occurred. Another test of an Australian link is whether or not an organisation *carries on business in Australia* (Privacy Act: 5B.2-3). This was modified in a post-GDPR revision, to better account for internationally trading companies who simultaneously offer goods and services to multiple markets (APP: B.18), as well as to include commercial activities conducted by non-profit organisations, rather than only for-profit actors (APP: B.16). In this sense, the Australian regime has moved somewhat closer to the standards outline in Article 3 of the GDPR in its treatment of external actors, but does not quite meet this standard as such.

General Principles for External Transfers

The underlying principle for external transfers under the GDPR is that none the rights provided to individuals by Regulation are undermined, including by onward transfers from one third state to another (GDPR: art. 44). This is supplanted by a recognition the international data flows are necessary for facilitating international trade, but the primary concern remains the protection of individuals, despite the need for trade and cooperation (GDPR: rec. 101). By contrast, while the

Privacy Act also recognises these two concerns, they are placed in equal esteem, as a goal of the Privacy Act is to '*facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected*' (Privacy Act: 2A.F). In this sense, the Privacy Act's explicit objectives offer a more equal balance between economic and normative concerns, where the GDPR's balance between these tends somewhat more toward the normative concern of rights protection. In keeping with this, where Article 44 of the GDPR is explicit about preventing the undermining of rights by onward data transfers from one state to another, the Australian regime has no such provision. Indeed, the only reference to such a situation is that the automatic routing of Australian data to one external state, via servers in another, would not constitute a *disclosure* of data to the intermediary state, but rather is a legitimate *use* of that data by the original APP entity (APP: 8.11). This is further evidence of a lower standard of rights protection in the Australian regime than its European counterpart. Again, this is an area more Europeanisation may have been expected under the Brussels Effect, given the problem such onward transfers could cause for trade with the EU already discussed.

However, despite there being no post-GDPR changes in the explicitly stated goals of the Privacy Act, amendments since the completion of drafting of the GDPR in 2016 have given greater legal protection to data subjects in the context of cross-border transfers. The most substantive of these was brought in by the *Notifiable Data Breaches Amendment* (NDB 2017). The core of this, is that where an eligible data breach occurs, APP entities are required to give written notice to both the data subjects in question and the Office of the Information Commissioner (NDB 2017: 26.WK). Concerning international data transfers, there are two key eligible breaches. The first is where an overseas recipient of data from an authorised transfer causes a data breach (Privacy Act: 26.WC), while the second is where an unauthorised international data transfer occurs in contravention of existing regulations, including APP8 (Privacy Act: 26.WE.2). In either instance, the original APP entity is required to notify any data subjects who may come to harm, and the information commissioner, wherein the latter may choose to investigate and take enforcement action. This is broadly similar to the notification requirements brought in by the GDPR in the EU regime (GDPR: rec. 87). On the whole, this represents a major strengthening of the Australian data protection regime with regards to cross-border transfers. This increase in the level of protection offered in the context of international data transfers is fairly strong evidence of policy transfer from the EU, both in the sense that this is a characteristic of a greater emphasis on the rights of data subjects than on the needs of businesses, which is broadly unique internationally to the GDPR, and in the sense that it occurred so expeditiously after the GDPR's final drafting.

Additionally, the Australian regime differs somewhat from the GDPR in its definition of overseas recipients. That is to say, the GDPR treats any transfer of personal data to another territory or international organisation as going to an overseas recipient (GDPR: art. 44). However, the APP does not recognise transfers to another jurisdiction, but within the same organisation, as an external transfer, and this is therefore not subject to either the APP or Privacy Act (APP: 8.6). This allows APP entities to transfer data to overseas offices or processing centres, where these are part of the same corporate entity. It does not however, allow similar transfers to related corporate bodies without taking additional steps. This distinction has been in place since 2012 (Privacy Amendment 2012: I.33). While the GDPR is undoubtedly stricter here, in the sense of being more restrictive of external transfers within the same corporate body,[3] this does not necessarily represent a lack of functional equivalence. While transfers within the same corporate body are not treated as external transfers as such, these bodies remain APP entities, and their overseas arms are therefore still subject to the Australian regime. Data subjects are then still afforded the same level of protection and access to enforcement as if the corporate body in question transferred their data between different locations within Australia. The only exception to this, in terms of protection, is where an Australian corporation transfers personal data to a jurisdiction with lower standards of security or rule of law, making breaches more likely. However, these companies are disincentivized from doing so as they would remain liable if such a breach occurred. In this sense, there is only a minor functional difference between the two regimes, and Europeanisation has not occurred post-GDPR in the framing of overseas recipients.

Transfers on the Basis of an Adequacy Decision

Under the GDPR, actors may transfer to third states without taking any additional safeguards, where the Commission has published a Decision that the third state in question provides adequate protection (GDPR: art. 45). No such central adequacy test exists in the Australian regime. Instead, individual actors are allowed to effectively, self-regulate and disclose data to external actors where they reasonably believe that they are subject to equivalent protections, and can provide enforcement mechanism to data subjects (APP: 8.19). This may either take the form of adequate protections offered by the recipient state, or by the recipient actor. However, it is stipulated that a substantial similarity is a question of fact (APP: 8.24), and can therefore be overruled by the Information Commissioner, where the APP entity would then be liable for enforcement action for an

[3] Where, as discussed later, they would be subject to the provisions concerning *binding corporate rules* (GDPR: art. 47).

infraction, which would then preclude other entities from transferring to the jurisdiction in question on the basis of substantial similarity. The specific requirements for assessing similarity include the presence of legislation or corporate schemes which provide equivalent or higher protection for data subjects, as well as the existence of independent supervisory authorities (APP: 8.24; APP: 8. 25), and are as such not dissimilar to the criteria for an adequacy decision from the Commission (GDPR: rec. 104). In this sense, the Australian Regime only falls short of European standards in its lack of centrality, and its presupposition of equivalency in the absence of a decision to the contrary.

Transfers According to Appropriate Safeguards

Under the GDPR, one of the primary safeguarding mechanisms concerning cross-border transfers concerns the contractual relationship between the exporting data controller and the recipient. This can either take the form of standard contractual clauses inserted into contracts between private actors, or legally enforceable agreements between public bodies (GDPR: art. 46. 2.a-c) The former can comprise either *standard contractual clauses*, published by the Commission, or approved by the relevant national supervisory authority and the Commission to the effect that their actions will not undermine the rights afforded to data subject by the GDPR (*ibid.*). In terms of substance, these include a third-party beneficiary clause, to allow data subjects to exercise contactual rights without being party to the contract, and a stipulation that the receiving actor is willing to be subject to the authority of to data protection authority and courts in the exporting controller's territory (FRA 2018: 261). Similarly, the Australian regime utilises the contractual relationship between APP entities and external actors as a primary method of safeguarding the rights of data subjects. However, substantial differences remain. Specifically, while the goal of contactual safeguarding under the Australian regime is to ensure that the external entity complies with the APPs, the entity does not become directly subject to the authority of the Australian Information Commissioner or courts. Rather, the APP entity is responsible for monitoring the external entity (APP: 8.17), and the APP entity itself remains liable for enforcement action undertaken by the Australian authorities. Additionally, no standard contractual clauses are published by the Australian authorities. In this sense, the use of contractual safeguarding under the Australian regime continues to be less centralised than that of the EU, both in the absence of standardised clauses, and in continuing to only take enforcement action against APP entities, rather than subjecting external controllers and processors to its authority.

One important post-GDPR change to the the use of contractual safeguarding under the Australian regime relates to breach notification. Even in the pre-GDPR version of the APPs, it was

stipulated that contractual arrangements between APP entities and external entities should contain a notification mechanism, whereby the the external entity is required to notify the APP entity of suspected or actual data breaches, and the remedial steps to be taken thereafter (APP: 8.16). While the text of this has not been amended, its implications for data subjects have substantially changed, due to the Notifiable Data Breaches amendment to the Privacy Act, as discussed previously. The crux of this is that, where previously contractual safeguarding only required the external entity to notify the APP entity of data breaches, the APP entity is now required to then notify the Information Commissioner and any implicated data subjects of this breach, on receiving notification from the external entity (NDB 2017). The authorities may then choose to take action against the APP entity directly, and the data subjects concerned may seek legal remedies. In this sense, the protection offered by contractual safeguarding has clearly been strengthened, particularly with regards to the enforcement and access to effective legal remedies for data subjects, even though the text outlining the requirements of these has not itself changed.

An alternative means of safeguarding under both regimes is the implementation of *codes of conduct* by external entities. There is little difference between the two regimes in terms of the substance of these. Each regime stipulates that codes of conduct should bind external actors to the same core principles and definitions as are applied internally (GDPR: art. 40.2; APP: 8.24), as well as requiring that data subjects have access to mechanisms to effectively enforce their rights (GDPR: art. 40; APP: 8.25). However, key differences remain between the two regimes. Under the GDPR, industry codes of conduct must go through an approval process, which in the context of external transfers requires the input of both national supervisory authorities and the Commission (GDPR: art. 40.6-9). Monitoring of codes of conduct which have been approved is then a joint process between the supervisory authorities in the third state and those within the EU (GDPR: art. 41.4). By contrast, the Australian regime applies the principle of substantial similarity to to codes of conduct for external entities, wherein APP entities may make transfers to these if they reasonably belief that the code offers the same level of protection to data subjects (APP: 8.23). APP entities could continue to transfer to external entities on this basis until a judicial decision is made to the contrary. In this regard, where the two regimes may be similar with regards to the substance and contents of the codes of conduct which they utilise, the EU regime is undoubtedly more stringent that its Australian counterpart in requiring approval to be given before external transfers are given on the basis of codes of conduct. In this specific regard, no Europeanisation can be observed.

Binding Corporate Rules

A similar situation can be seen in the two regime's respective treatment of external transfers on the basis of *binding corporate rules*, which are adopted by groups of related enterprises. Under the GDPR, these are required to contain all 'essential principles and enforceable rights' to ensure that the rights of data subjects are not compromised by transfers within such groups of enterprises (GDPR: rec. 110). This is then monitored by a designated supervisory authority from the member state most connected with the group of enterprises (GDPR: art. 47.2.h). The entity within the group of enterprises must also accept liability for any breach of the corporate rules (GDPR: art. 47.2.j). The corporate rules must thereafter be approved by the competent supervisory authority, in cooperation with the European Data Protection Board (EDPB) (FRA 2018: 263). As with safeguarding via codes of conduct, binding corporate rules under the Australian framework are subject to the logic of reasonable belief of substantial similarity. However, in the instance binding corporate rules, a single concrete test is stipulated for this similarity. Specifically, it is actually stated that these should be implemented in accordance with EU law on the issue of external data transfers (APP: 8.21). This was present in the original text of the APPs, before the implementation of the GDPR. Indeed, there is even reference to the now-defunct Article 29 working party as a source of further guidance. In this sense, policy convergence has certainly occurred, as the substance Australian regime has explicitly changed by virtue of the EU regime changing. However, while this is undoubtedly an instance of the European regime being projected, it would be spurious to describe it as externalisation. Rather, it has more in common with the imitation mode of Europeanisation, as detailed in the first chapter of this thesis.

Enforceability of External Judicial Decisions Outside of Internal Law

The Australian and EU regimes differ in their approach to legal decisions within third states which would require domestic entities to export data. In essence, the GDPR only recognises such decisions where an international agreement exists between the EU and the third state to that effect (GDPR: art. 48), or where the requirements of Chapter V are otherwise met (GDPR: rec. 115). Under the Australian regime, the picture is somewhat more complex and situational. One crucial element of this is its different treatment of private and state actors. Private actors within Australia may only export data because of a foreign judicial decision where there is a requirement under Australian law for them to do so, for instance as part of an international agreement on international crime (APP: 8.35-5). Arms of the Australian state are permitted to transfer data to a third state without complying with the APPs where this is *authorised* or *required* by an international agreement (APP: 8.47). While this may appear to be a semantic difference, the distinction is nonetheless important. The reason for this is that state agencies may carry out an international

transfer where it is authorised by Australian law as part of its international commitments, without necessarily being required, so long as the agency itself reasonably beliefs that the transfer is necessary and the recipient is a body which carries out equivalent functions (APP: 8.52). In drawing such a distinction between private and state actors the Australian regime continues to be less uniformly applicable than that of the EU under the GDPR.

Additionally, the APPs stipulate that where an overseas recipient of data from an APP entity is required by their domestic legal system to disclose this data as part of an enforcement process, then this will not be considered a data breach for which the APP entity is accountable (APP: 8.60-3), although it is recommended that the APP entity notifies the data subject in question and explain that this does not constitute a data breach, where the APPs have otherwise been complied with (APP: 8.63). This specific situation is not addressed by the GDPR in its treatment of overseas judicial decisions or enforcement actions. This is unlikely to be of particular concern in the instance that the overseas recipient has received the data in question on the basis of an adequacy decision from the Commission, as there would therefore necessarily be sufficient rule of law and protection for the data subjects in question in terms of when and how their data can be disclosed to government authorities. However, in the instance that the original transfer was made on the basis of one of the other safeguarding mechanisms outlined above, the situation would be somewhat more ambiguous both in terms of whether a disclosure to the third-state authorities is permissible by the recipient, and in terms of whether or not the original EU entity is accountable if this where to be considered a breach. As this is not addressed explicitly, except in acknowledging that one jurisdiction seeking to extraterritorially impose its own laws on another in this way may be problematic under international law (GDPR. rec. 115), it would in all likelihood come become a political matter between the EU and the third state, as the EU does not have the legal ability to prevent authorities in third states from applying their own laws within their own jurisdictions.

Derogations for Specific Situations

Both the Australian and EU regimes allow for derogations to the safeguarding requirements outline above in certain exceptional circumstances. While there are factors common to both regimes, important differences also exist between them in this regard. The first derogation common to both regimes is in the instance that a data subject has expressly consented to an international transfer taking place in the absence of any standard safeguarding (GDPR: art. 49.1.a; APP: 8.27). In both instances, consent may permit ongoing transfers to the same external entity for a particular stated purpose, and general or unlimited transfers of this kind cannot be legitimately consented to (GDPR: rec. 32; APP: 8 .32). However, an important difference in this regard is that derogations

under the GDPR may only justify external transfers in exceptional and limited individual cases, and data subjects' consent should therefore not be used as a basis for large-scale data transfers (FRA 2018: 264). No such stipulation exists under the Australian regime, meaning that consent would be a legitimate basis for mass data transfers, provided that all subjects involved have consented. A related difference is that the GDPR lists the fulfilment of a contract entered into by, or in the interest of a data subject as a legitimate derogation (GDPR: art. 49.1.b-c). This derogation does not exist under the Australian regime, and consent would therefore still be necessary with regards to such contractual matters. In this regard, it is difficult to see convergence, as fairly large difference remain.

Additionally, both regimes apply derogations in cases of compelling public or individual interests. In the instance of protecting individual interests, the GDPR is somewhat vaguely worded, in applying this to either the data subject or another natural person, as well as in not specifying what constitutes a 'vital' interest (GDPR: art. 49.1.f). By contrast, the Australian regime only allows three specific instances where individual interests would be a justifiable basis for a non-APP external transfer. These are in the case of a serious threat to the health, safety or life of an individual, efforts to locate a missing person, or as part of an action against unlawful activity or misconduct (APP: 8.38-42; Privacy Act: 16A). In this regard, the Australian regime offers considerably more specificity with regards to what constitutes justifiable protection of individual interests. However, under the APPs, APP entities need only prove that they reasonably belief that such a transfer is necessary, and that seeking the consent of a data subject would be impractical or unreasonable, whereas the GDPR states that the individual concerned must be unable to give consent (APP: 8.38; GDPR: art. 49.f). Similarly, the GDPR stipulates that protection of public interest may take a number of forms, including regulatory, financial, social or security functions (GDPR: rec. 112). The APPs limit public interest derogation to those necessary for for diplomatic, consular or defence forces activities (APP: 8.43-46; Privacy Act 16A). Again, it is clear that major differences remain between the two regimes with regards to permissible derogations surrounding international transfers. This is particularly notable, given that this is an area which could greatly affect the ability of entities to circumvent each regime with the use of onward transfers, and so some degree of Europeanisation or convergence would have been expected.

International Cooperation for the Protection of Personal Data

Finally, the GDPR sets out the terms under which the EU Commission and national supervisory authorities engage and cooperate with third states and international organisations in the

field of data protection. This includes mutual assistance, policy exchange, consultation with industry and enforcement activities (GDPR: art. 50). By contrast, the Australian regime only concerns itself with such cooperation in terms of its membership of relevant international organisations, including the UN and OECD, and the obligations which come along with these (Privacy Act: Section 1: Preamble). However, in reality this is less a regulatory matter than it is a political one, especially with regard to how each market sees itself and its role in the world. Additionally, the EU, as an international organisation, has more reason to state the roles of its various components in this regard than Australia would as nation state. As such, it is unsurprising that a different approach is taken on this particular issue.

5. 2. Empirical Analysis: Canada

Case Background

Like Australia, Canadian initial efforts to protect its citizens' personal data stem from its obligations as a member of the OECD, with the passage of the *Privacy Act* in 1983 (Department of Justice 2017). Once again, this resulted in a regime which was solely applicable to government agencies and institutions at a federal level. A separate piece of federal legislation was later passed to protect data which is processed in the private sector, in the form of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2001. A number of federal states within Canada also have separate pieces data protection legislation. However, these only apply within the territory of these states, while PIPEDA applies to commercial data transfers across federal or national borders. As such, such state laws are outside of the scope of interest of this thesis. Importantly, the specific form and character of PIPEDA, and to a certain extent its existence, have already been shown to have been influenced by the 1998 EU Data Protection Directive (Bennet & Raab 2003). Once again, this previous instance of Europeanisation is clearly indicative of the salience of EU policy change to the Canadian regime. Like Australia, Canadian legislation has undergone substantive amendments post-GDPR. Additionally, the Office of the Privacy Commissioner (OPC) opened a consultation process in 2019, with a view to amending its guidelines on cross-border transfers, such that consent of the data subject is required in all circumstances. This change would have made the Canadian regime considerably more stringent than that of the EU, or any other market on this specific issue. However, after considerable criticism and concern from industry figures, this process was halted, on the basis that this model would be overly restrictive for businesses, without contributing much to the protection of citizens' personal data (OPC 2019).

Regulatory Regime and Governance of External Transfers

Through the Privacy Act and PIPEDA, external data transfers are dealt with by Canadian primary legislation. These are accompanied by guidelines from the OPC on this specific issue (OPC 2009). However, these are wholly explanatory, and do not in and of themselves create rules within the Canadian regime. Rather, they serve as official interpretations of the primary legislation, whereas the APPs, for instance, supplant primary legislation in the Australian regime. With regards to the issue of applicability, there are certain key differences between the EU and Canadian regimes. Perhaps the most obvious of these is Canada's usage of separate pieces of legislation for public and commercial actors, where the GDPR is, of course, generally applicable. One crucial side-effect of employing specific legislation for specific kinds of actors, rather than a single generally applicable

piece of legislation, is that certain actors do not fall within the categories provided for, and are therefore not subject to regulation. For example, since PIPEDA and the Privacy Act respectively apply to commercial and public actors, charitable and non-for-profit organisations, are not typically subject to either.[4] Nor are political parties or numerous other kinds of non-commercial private organisations. While this is of the Canadian regime as a whole, it is particularly problematic in the context of cross-border data transfers, especially given that non-commercial organisations are likely to handle sensitive data, for instance relating to political or religious affiliations. Since Canadian non-profits are effectively not regulated, they could easily be used as a vehicle for onward transfers of EU citizen's data, and therefore a certain degree of Europeanisation would be expected here, as data transfers to Canada could greatly undermine the goals of the GDPR in this respect.

On the topic of extraterritorial jurisdiction, little is said in Canadian primary legislation. Obviously, the Privacy Act, in only applying to government bodies, cannot apply to external actors. PIPEDA does not explicitly address this issue. However, case law has established the conditions where PIPEDA is applicable to overseas actors. Specifically, PIPEDA applies to organisations outside of Canada where their activities are related to a commercial activity, and where there is a *real and substantial connection* between the organisation and a potential complainant in Canada (*A.T. v. globe24.com:* 41). A real and substantial connection can take multiple forms. It may, for instance, exist in the case that significant operations take place in Canada on behalf of an organisation which is legally incorporated elsewhere, or which has overseas servers (OPC Report 2019: 51). A real and significant connection may also exist where an overseas company remotely collects or processes Canadian data, even if they have no physical or legal presence in the country (*A.T. v. globe24.com:* 5). In either instance, PIPEDA applies and the OPC has jurisdiction to take action against the organisation in question. In this regard, the Canadian regime is effectively somewhat similar in its applicability to external actors handling data, except for the requirement that this must be related to a commercial activity. While this principle isn't yet codified in legislation, it worth noting that it first emerges in 2015, 15 years after PIPEDA's entry into force (OPC Report 2015: 61), and during the drafting and consultation phase of the GDPR. While this does represent a certain amount of regime convergence, it is less easy to establish causality between the GDPR and the Canadian regime in this respect, due this development occurring before the GDPR was finalised. Indeed, it could be as likely to be the case that the two regimes came to the same regulatory solution more or less simultaneously.

[4] Except while they are carrying out commercial activities, for instance collecting membership fees (OPC 2019).

General Principles for External Transfers

As previously noted, the GDPR's stated fundamental principle for external transfers is to ensure that the rights of individuals are not undermined, while recognising as a secondary concern that international transfers are necessary for international trade and cooperation (GDPR: art. 43; rec. 101). Again, the Canadian regime also recognises these two aims, in the stated purpose of PIPEDA, referring to them as the right of privacy of individuals, and the need of organisations to collect, use and disclose personal information (PIPEDA: 3). Unlike under the GDPR, these are placed in equal esteem, and there is not qualification that the normative element of this takes precedence over the economic need to maintain free flows of personal data. In this regard, discrepancy remains between the Canadian regime and that of the EU with regards to their stated aims, and thus convergence has not occurred, in the sense that Canada has not undergone a shift towards a more normative underpinning of its data protection regime, where by contrast the EU does. Where article 44 of the GDPR makes explicit reference to the issue of personal data protection being undermined by onward transfers through multiple third states, PIPEDA makes no such stipulation. Again, this is an issue of particular salience in terms of the adequacy of a third-state regime, and as such this is one area where Europeanisation may have been particularly expected.

Again, while the stated purpose of the Canadian regime has not changed, there has nonetheless been a strengthening of the rights of individual data subjects which places more responsibilities on organisations, including with regards to external transfers. Specifically, the 2018 *Breach of Security Safeguards Regulations* (BSSR) amendment to PIPEDA brought in a requirement that data organisations should notify the OPC and affected individuals in the case of a data breach, as defined in PIPEDA as a breach of the required safeguards, or a failure of an organisation to implement these properly in the first place (BSSR 2018: 2.1; BSSR 2018: 3; PIPEDA: 2.1). In the context of external transfer, this could comprise either a failure of a domestic organisation to implement the required safeguards, which will be discussed later, or the non-compliance of an overseas actor which is subject to PIPEDA on the basis of a real and substantial Canadian connection. The intended effect in either case is that the OPC will then be able to investigate said breach, and concerned individuals can seek legal remedies. In this sense, there is a clear similarity between the Canadian breach reporting requirements and those under the GDPR, although the Canadian regime lacks the time requirements laid out in the GDPR, where breach notifications must be made within 72 hours (GDPR: art. 33; art. 34). In this sense, the rights of individuals have clearly been strengthened at the detriment of business' economic interests. Once

again, the timing of this instance of convergence is a strong indication of direct Europeanisation as a result of the GDPR coming into force.

Stark differences exist between the Canadian and EU regimes in their conceptualisation of overseas recipients. As noted before, under the GDPR the test for whether or not a transfer is considered external is the actual territoriality of the recipient (GDPR: art. 44). By contrast, PIPEDA does not explicitly differentiate between domestic and cross-border transfers of data. Rather, in all cases, organisations must ensure that recipients offer a comparable level of protection (PIPEDA: 4.1.3-4). Here, an implicit distinction emerges between domestic and cross-border transfers, in that domestic organisations will of course offer comparable levels of protection as the original organisation, by virtue of the fact that they are subject to the same laws. In the case of cross-border transfers, where the recipient is therefore not directly subject to Canadian laws, the organisation will therefore have to make the additional safeguarding steps which will be outlined shortly. The original organisation in control of personal data is wholly accountable for the actions of third parties which process said data, and is therefore liable for enforcement action under PIPEDA (PIPEDA: 4.1.3). In not explicitly addressing cross-border transfers in this way, the Canadian regime offers a far greater scope for individual organisations to self-regulate in this regard, offering far less stringent or centralised requirements. Again, this is a particular area where Europeanisation may have been expected, as more self-regulation necessarily makes it more difficult for onward transfers of EU to countries with lax data protection regimes may occur via Canadian organisations.

Transfers on the Basis of an Adequacy Decision

An additional effect of PIPEDA not explicitly distinguishing between internal and external transfers is that it also does not distinguish between external jurisdictions in terms of the protections offered under their regimes. Indeed, the OPC note that where the EU takes a state-to-state approach to external transfers, the Canadian regime is built on an organisation-to-organisation model (OPC 2009). The Canadian authorities therefore do not assess the adequacy of external jurisdictions, and therefore transfers cannot be made without safeguards to certain jurisdictions on the basis of their internal data protection regime. On the one hand, this makes the Canadian regime much more uniform in its treatment of external recipients of data, in the sense that the same safeguarding requirements are required across the board. On the other, there is potential that this approach opens up security risks of its own. For example, an effect of the EU's adequacy approach is that businesses are encouraged to transfer data to third states with high standards in terms of stability, rule of law and administrative capacity, by eliminating the need to undertake safeguarding measures in this instance. By contrast, the Canadian regime offers no such incentive, and organisations may

then be incentivised to transfer Canadian data to the cheapest jurisdictions, which may have lower standards of stability or rule of law. In either case, while the Canadian regime is undoubtedly more uniform in its treatment of external jurisdictions, it is at the same time far less centralised in not giving the authorities the power to make it easier to transfer to certain jurisdictions than it is to others on the basis of the protection offered by their domestic regimes.

Transfers According to Appropriate Safeguards

As with under the GDPR, one of the primary means of safeguarding the rights of data subjects during and data transfer, including international transfers, under PIPEDA. However, there are several important differences between the two regimes. Unlike in the EU, no standard contractual clauses are provided by the Canadian authorities. Additionally, the contractual language involved does not need to include third-party beneficiary clauses, or stipulations that the receiving entity become subject to the Canadian authorities. Rather, the requirements for contractual relationships between Canadian organisations and third parties should include guarantees that the third party has comparable policies in place, along with appropriate staff training, complaints processes and the right of the Canadian organisation to conduct ongoing audits of these practices (PIPEDA: 4.1.3-4). As the third party does not become subject to the Canadian authority's jurisdiction, it is worth noting that the Canadian organisation remains liable for any breaches under the accountability principle (PIPEDA: 4.1.1). This does not, however, preclude them from placing some contractual liability on the third-party organisation, such that they may recoup damages from them in the instance of a breach stemming from their own failings or malpractice. Indeed, the OPC's guidelines suggest that organisations act in their own best interest in this regards, as well as upholding the rights of data subjects (OPC 2009). Once again, in retaining an organisation-to-organisation approach and a great degree of self-regulation, the Canadian regime remains distant from that of the EU in this specific regards.

While the specific requirements for contractual safeguarding have not changed in the Canadian regime post-GDPR, it is also worth considering how the impact of these safeguards on individual data subjects has been affected by the BSSR amendment. In one sense, this has had a fairly limited impact. Third parties are not themselves required to notify the authorities or concerned data subjects of data breaches under BSSR. Instead, the Canadian organisation remains responsible for this (OPC 2018). Additionally, unlike the GDPR or APPs, contractual safeguarding under PIPEDA does not necessarily require clauses that the third party must notify even the Canadian organisation of data breaches, although organisations may, of course, choose to include these. In the absence of this, the onus remains on the Canadian organisation to audit and inspect the

third party, and then subsequently notify the authorities and concerned individuals where it identifies a breach, so that the former may undertake enforcement action and the latter may seek legal remedies. Even in this instance, the caveat remains that it is only required to do so in the case of potential for real and significant harm to data subjects. In this sense, while the impact of contractual safeguarding under PIPEDA has undoubtedly been altered somewhat by the post-GDPR BSSR amendment, this impact is relatively minor in the sense that the extent to which individual data subjects benefit from it remains contingent on the activities of the controlling organisation and the potential for harm to the individual, rather than being the automatic right that it is in the other two regimes under examination. As such, a comparatively small degree of convergence can be said to have occurred.

Unlike the GDPR, PIPEDA does not explicitly mention *codes of conduct* as a safe-guarding mechanism. However, this does not necessarily preclude their usage. Indeed, the exact language which applies to safeguarding of international transfers says that organisations should use '*contractual or other means'* to ensure comparable levels of protection are offered to data subjects by external entities (PIPEDA: 4.1.3). There is therefore no mechanism for approving codes of conduct, as is employed by the EU authorities. In essence, these would contain the same requirements as contractual safeguarding, to the effect that the same level of protection is offered to data subjects, including in terms of internal policies, staff training and the ability of the Canadian organisation to audit these, where the Canadian organisation remains accountable for the conduct of the third party, and therefore solely liable for enforcement action. In this sense, the Canadian regime is somewhat agnostic with regards to the form of safeguarding which is employed in allowing individual organisations great scope to choose this for themselves, on the basis that they themselves are solely accountable for the outcomes of these. While some post-GDPR consultation work has begun by the government on strengthening the Canadian regime in this regard, including introducing more specific and centralised requirements for codes of conduct (ISEDC Proposal 2019), at present no changes have been forthcoming, and as such no Europeanisation can be said to have occurred.

Binding Corporate Rules

Similarly, no references are made to *binding corporate rules* in either Canadian legislation or the guidelines which accompany it. However, the use of these is recognised is recognised by the OPC and relevant case law. The effect of these findings is that contractual safeguarding is not required in the case of related corporate bodies transferring Canadian data across borders, so long as they are subject to the same levels of data protection (OPC Investigation 2006). In essence, this

means through the use of binding corporate rules, although this is not stated as such, and that these represent a legitimate example of 'other means' to ensure comparable protections are offered to Canadian data subjects. Additionally, the Canadian arm of the group of related organisations remains accountable and subject to the Canadian authorities (PIPEDA: 4.1.3). As with codes of conduct, no specific additional requirements exist for safeguarding through binding corporate rules beyond those which have been outlined already. Unlike under the GDPR, there is no centralised approval mechanism for binding corporate rules in the Canadian regime (GDPR: art. 47), although these may in theory be deemed to be inadequate at a later date by the OPC. In this sense, although both regimes recognise the use of binding corporate rules to safeguard the rights of data subjects, the Canadian regime continues to lag behind its European counterpart in its lack fo centrality and standardisation. Additionally, where policy consultation documents have recognised the need for increased oversight and centralisation with regards to safeguarding via codes of conduct, the same is not the case with regards to binding corporate rules (OPC Proposal 2019).

Enforceability of External Judicial Decisions Outside of Internal Law

As established earlier, under the GDPR EU entities may only disclose data to foreign authorities outside of the other requirements of Chapter V in the instance of an international agreement existing between the EU or member state and the third state in question (GDPR: art. 48; rec. 115). Under PIPEDA, organisations may transfer data to foreign authorities without the consent of data subjects where this is necessary for a legal investigation or enforcement activity and the authorities in question have identified the legal basis for them to acquire this data (PIPEDA: D1.7.3.C.1.ii), or when the organisation is issued with a subpoena from a court or body with jurisdiction to compel the organisation to disclose information (PIPEDA: D1.7.3.C). In practice, a foreign court or institution could only have a legal basis for compelling a Canadian organisation to disclose data in this way as part of an international agreement to that effect, or as through Canada's membership of an international organisation, such as the International Criminal Court (ICC). However, in either case it is more likely that foreign authorities would be required to make a such a request for a disclosure through the Canadian authorities, rather than directly to the organisation in question. Similarly, under the Privacy Act, Canadian authorities are permitted to disclose data to foreign courts and authorities on the basis of an international agreement or Canada's membership of an international organisation, or when issued with a subpoena by a body with jurisdiction to do so (Privacy Act: 8.2.C; 8.2.F). In this sense, little practical disparity existed between the Canadian and EU regimes pre-GDPR, and as such no Europeanisation can be observed.

Derogations for Specific Situations

Once again, as PIPEDA does not explicitly differentiate between international and domestic data transfers, it is necessary to consider the situations where organisations may make data transfers without the consent and knowledge of data subjects, outside of the ordinary requirements. As with under the GDPR, many of the circumstances in which international data transfers may occur without the data subjects consent or knowledge involve their personal well-being. These include data which is necessary to identify an individual who is ill, injured or deceased, as well as that which is necessary to prevent or investigate financial crimes against a person (PIPEDA: 8.3.D.3-4). However, in either case such a transfer may only be made to a government institution, the individual in question's next of kin, or another person they have authorised. Such qualifications do not apply in the GDPR. Similarly, data transfers may be made without consent or knowledge of the data subjects in the case of a threat to the life, health or security or an individual (PIPEDA: 8.3.E). This however may be done to any kind of receiving entity, on the condition that the Canadian organisation notifies the concerned data subjects about the disclosure. Again the two regimes are different in that PIPEDA refers to very specific circumstances, where the GDPR allows derogations in instances of individual or public interest more generally. Additionally, while there is some commonality in terms of derogations, there are also multiple situations under the GDPR where safeguarding is not required which are not recognised in the Canadian regime. For example, under the GDPR cross-border transfers can be made in the absence of other safeguards, with the consent of the data subject (GDPR: art. 49.1.A), or in certain cases where this is necessary to fulfil a contract (GDPR: art. 49.1.B). On the whole, no particular policy convergence can be observed with respects to derogations.

International Cooperation for the Protection of Personal Data

Again article 50 of the GDPR sets out the basis on which the Commission and national authorities should engage with their international counterparts in third states and international organisations to cooperate in the field of data protection. While it has been noted that this is as much a political concern as it is a regulatory one and that it is also tied to the internal dynamics of the EU itself, it is still worth considering the similarity in this regard across regimes. Similarly, the role of the OPC is laid out in PIPEDA, including its responsibility to cooperate with international counterparts to develop instruments to further the protection of individuals' data, both domestically and abroad (PIPEDA: 23.2.C). It's aims and activities in this regard occur in particular with regards to emerging technologies and their impact on personal data protection (OPC 2015). In this sense, the two regimes do not appear dissimilar in their disposition towards international cooperation. While no convergence can be seen towards the GDPR's more detailed provisions on this specific

topic, to some extent this is to be expected in the issues specificity to the EU, and so Europeanisation is less likely here.

5. 3. Empirical Analysis: Discussion

On the whole, both cases have exhibited low levels of convergence with the EU regime with respect to cross-border data transfers. Indeed, the extent of Europeanisation which has occurred appears to quite neatly fit the *absorption* model, where a limited number of European policy features are incorporated into the domestic regime, without any substantive changes to the domestic policy structures (Orbie & Carbone 2016). What is striking however, is the similarity in the the policy areas which have been absorbed in each case. Specifically, two broad instances of convergence have occurred in each. The first relates to breach notifications, which became mandatory in certain instances in each case after the entry into force of the GDPR, where in EU law these were previously advised rather than mandatory. While not only applicable to cross-border data transfers, these changes have a substantial impact on the effect of the required safeguards in this specific field in each case, especially in improving the ability of the authorities to investigate breaches which have resulted from safeguards not being properly implemented, and that of data subjects to seek legal remedies where these have occurred. In both cases however, this represents a change in the impact of safeguarding, rather than an overt change to the safeguarding requirements themselves. However, in practical terms, this has a somewhat different impact across the two regimes in terms of their safeguarding requirements for international transfers. The core of this is that under contractual safeguarding requirements in Australia, APP entities are required to include mandatory notification clauses in contracts with external third parties, whereas under the Canadian regime, the onus is on Canadian organisations to audit external third parties to identify breaches, where in either case the domestic company is then subject to their mandatory breach notification requirements. In this regard, the impact on changes to notifiable breach requirements in Australia on contractual safeguarding bring it somewhat closer to the EU requirements than is the case in Canada, although the difference is somewhat marginal.

The second instance of convergence which is common to both cases relates to the extraterritorial applicability of their data protection regimes. As discussed, the GDPR is novel in its application to any organisation processing the data of subjects located within the EU (GDPR: art. 3.2). In both cases, movement can be seen towards a similar extraterritorial applicability. In the Australian regime, this has involved an expanded definition of what constitutes an *Australian link* post-GDPR, while in Canada this has taken the form of the OPC introducing the idea of a *real and substantial connection* in their opinions of the extraterritorial applicability of PIPEDA during the drafting period of the GDPR, and the subsequent application and development of this concept

through case law to essentially resemble the GDPR's extraterritorial applicability (*A.T. v.* globe24.com). In both cases, an increase can be seen in the extent of extraterritorial applicability assumed by the domestic authorities, towards that provided for under the GDPR. In the context of cross-border data transfers, the impact of this is obviously significant in bringing a greater number of international actors under the jurisdiction of each regime, which in turn affects their ability to protect their citizens' data in an increasingly globalised market for services. In both cases, this change has taken the form of the behaviour and international ambitions of the authorities in each case, rather than a concrete legislative change.

Beyond these two instances of convergence, little Europeanisation can be observed across the two cases[5]. Indeed, where Europeanisation does appear to have occurred and European regulatory practices have been absorbed, this has happened with regards to the same regulatory areas and approaches. In addition to that, there appears to be little substantive difference between the extent of Europeanisation even within these regulatory areas. In this sense, it does not seem that the hypothesis that this would vary as a function of each case's relationship with the Single Market in terms of trade in services applies, or that the significance of the EU market to the economy of each case in this respect is the explanatory factor which determines the extent to which Europeanisation occurs in interdependent markets in the field of data protection. The following chapter comprises concluding remarks, including on the implications of this result.

[5] As referred to previously, the Australian requirements for binding corporate rules have changed by virtue of changes to these under the GDPR, but this is contingent on the authorities' previous decision to tie their requirements to those of the EU. As such, it is somewhat incidental to the analysis at hand.

6. Conclusions

The goal of this thesis was to investigate to what extent policy convergence is occurring internationally in the field of data protection, as a result of the economic and regulatory power of the EU, by specifically examining whether Brussels effects have occurred in this domain in Canada and Australia. Where Europeanisation had previously been empirically observed in individual cases, this thesis sought to apply positivist cross-case analysis to two states were Europeanisation was likely to occur in this regulatory area to establish the predictive power of this strand of the Europeanisation theory, whereas previous within-case analysis has simply sought to determine whether or not Europeanisation has occurred after the fact. The theoretical grounding of this was the framework of Europeanisation via externalisation and the Brussels effect, wherein other jurisdictions adopt regulations which are similar to those in the EU because of the presence of internationally trading companies. Existing empirical work had suggested that this effect occurred in the cases in question with regards to the previous EU data protection regime, and so they were the ideal vehicle to further test and develop this theory. From this existing theoretical framework, the expectation emerged that the more significant the EU market is to export-orientated domestic companies, the more their data protection regime is likely to become Europeanised.

To examine how this theoretical expectation plays in the real world, a small-N comparison was applied to the cases of Canada and Australia, utilising a most similar systems design. These cases were selected, in part, because they meet the theoretical criteria for a Brussels Effect to occur, in both being large, economically developed states, which are outside of the EU's direct sphere of influence, but nonetheless retain moderate trade interdependence. They do, however, vary in terms of the significance of the EU market to export-orientated companies, as an inverse of their respective trade-in-services deficits with the EU, with Canada consistently displaying a smaller deficit over the past decade. To ascertain respective levels of Europeanisation, the empirical portion of this thesis analysed each cases' provisions on cross-border data transfers, with specific emphasis on the safeguarding mechanisms which are required by organisations within each jurisdiction, as well as their extraterritorial functioning. The rationale for choosing this specific area of regulation relates to it being particularly pertinent to internationally trading companies, and therefore and area where Europeanisation via the Brussels Effect would be most expected. This analysis took account of primary legislation, official guidance from relevant authorities in case law, with a view to establishing which elements of the regulatory regime in each case had substantially converged

towards the EU regime post-GDPR, with the theoretical expectation that more Europeanisation would be observed in the case of Canada than in Australia.

In both cases, a low, and indeed somewhat negligible level of Europeanisation was observed, falling into the category of policy absorption. Additionally, the specific regulatory elements which were Europeanised were common to both regimes. Specifically, these are an increase in the extraterritorial jurisdiction assumed by the authorities in each regime, and the strengthening of the impact of of certain safeguarding mechanisms for cross-border transfers, virtue of the introduction of mandatory breach notification requirements more generally, although the latter may be considered somewhat incidental to separate regulatory changes, in not addressing international data transfers explicitly. The fact that, to the extent that Europeanisation is observable, both cases absorbed the same policy elements indicates a common impetus for these policy changes. However, the lack of variation in the extent of Europeanisation, within a given policy element or otherwise, falsified the hypothesis that more Europeanisation would occur as a function of differing trading relationships with the EU. That is, in this instance, a greater significance of the EU market to export-orientated companies did not result in a higher degree of Europeanisation occurring, as was predicted by the theoretical literature. Of course, it is necessary to consider some of the potential reasons why this is the case, and the implications of these.

One element of this is temporal. That is to say, that there is little in the theory that indicates that Europeanisation via the externalisation or the Brussels Effect would occur instantaneously, or on a wholesale basis. Rather, it is perfectly possible that Europeanisation would occur gradually through the absorption, adoption and transformation stages. Indeed, regulatory change is a laboured, multi-actored and slow process, as can be seen in the multiple Canadian policy consultations which were referred to earlier. In this regard, it is also plausible that Europeanisation in one case may out-pace that of the other at some point in the future, which would require renewed empirical work at some point in the future. However, this does not seem particularly likely to be the case here, as several years after the GDPR was finalised, one would expect at least some variation between the cases in the extent that they have become Europeanised. In the absence of this, revisiting the same theoretical hypothesis at a later point would likely be unproductive, as there is little reason to suspect at the current moment that a different result will be observed.

What is more likely is that this null result indicates a limited predictive power of externalisation of the Brussels effects as modes of Europeanisation. Of the minor regulatory change which can be seen in both cases, one of the only areas of change relates to the extra-territorial ambitions of the domestic authorities. That is to say, where there has not been substantial

convergence towards the EU approach to safeguarding international data transfers, there has been an increase in the scope to which authorities in each of the cases seek to apply their own regimes to external actors. This is contradictory to the expectations of externalisation or the Brussels effect, in the sense that it is a clear instance of third states seeking to assert their own regulatory preferences on the international stage, rather than simply converging towards European standards with little or no agency being displayed. Indeed, this further contradicts the theoretical expectations under examination, in the sense that this development would presumably be contrary to the interests of internationally trading companies, as an international environment with multiple contradictory extra-territorial regimes would be a more difficult one to operate in. In this sense, externalisation and the Brussels effect seem not only to lack predictive power, but to be contradicted by the empirical facts entirely.

Of course, in the context of a null finding it is always worth reflecting on the limitations of the research itself. In this instance, one key limitation relates to the the research design in this thesis. As has been noted, small-N comparisons, of the kind employed here, are sometimes derided in their limited ability for making generalisable inferences. That is to say, that the fact that externalisation and the Brussels effect were unable to predict regulatory change in this policy field and in these cases does not necessarily mean that the same would be true of other cases or within other policy fields. Indeed, it is perfectly plausible that a large-N comparison of cases in the field of data protection may have yielded another result. However, given that treating regulatory change as a dependent variable is a laborious and manual process, it is difficult to see how this would be achievable. Additionally, finding the required cases for a large-N comparison of this kind would likely be very challenging. As such, it remains the most convincing and practical strategy to select cases where the theory and previous empirical scholarship indicates that Europeanisation is most likely to have occurred to representatively assess the power of externalisation and the Brussels effect to predict regulatory change more generally.

As noted, the goal of this thesis was to investigate the extent to which the EU's regulatory and economic power led to it exporting its regulatory regime in the field of data protection. To do this, the most plausible economic mechanism of Europeanisation was chosen and subjected to empirical testing. In the course of doing so, this thesis has contributed to the Europeanisation literature, in demonstrating this mechanism to be insufficient to explain the dynamics of Europeanisation at play in the field of data protection, in the sense that it does not appear to have any predictive power, even when its own stated conditions are met. Where previous scholarship has observed Europeanisation in third-state data protection regimes and ascribed it to the Brussels

Effect, this cross-case analysis has shown that a renewed framework is necessary to properly understand how Europeanisation occurs. However, the original urgency for studying the international regulatory dynamics concerning data protection remain, given that this is a regulatory issue which is so novel in its trans-nationality. Indeed, this thesis has shown a renewed urgency both in displaying that, rather than converging, the cases under examination are are increasingly seeking to apply their own existing regimes externally, and in exposing a lack of predictive power in one of the approaches to regulatory change which might have most plausibly applied in this policy area. In light of this, this thesis has made a substantial contribution in exposing such a short-coming in the Europeanisation literature, and the need to approach to issue of policy transfer in the field of data protection through other lenses. In light of these findings, the most relevant of these will likely be that of traditional inter-state power dynamics and bargaining, either bilaterally or through international organisations, as well as the roles of international corporations themselves in shaping the international regulatory environment in which they will operate in the coming years.

Bibliography

Aaronson, S. A., & Leblond, P. (2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law*, *21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Attorney-General's Department. Retrieved 10 March 2020, from https://www.legislation.gov.au/Details/C2017A00012/Html/Text, http://www.legislation.gov.au/Details/C2017A00012

Albrecht, J. P. (2016). How the GDPR Will Change the World Forword. *European Data Protection Law Review (EDPL)*, *2*(3), 287–289. https://heinonline.org/HOL/P?h=hein.journals/edpl2&i=313

Anckar, C. (2008). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *International Journal of Social Research Methodology*, *11*(5), 389–401. https://doi.org/10.1080/13645570701401552

Archie, L. (2005, March). *Hume's Considered View on Causality* [Preprint]. http://philsci-archive.pitt.edu/2247/

A.T. v. Globe24h.com, 4 FCR 310 (Federal Court, Canada 2017). http://canlii.ca/t/gx6bl

Australian Government. (n.d.-a). *Privacy Act 1988* (au). Office of the Australian Information Commissioner. Retrieved 8 March 2020, from http://www.legislation.gov.au/Details/C2018C00034/Html/Text

Australian Government. (n.d.-b). *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (au). Attorney-General's Department. Retrieved 10 March 2020, from http://www.legislation.gov.au/Details/C2012B00077/Explanatory Memorandum/Text

Australian Government. (n.d.-c). *Privacy Amendment (Notifiable Data Breaches) Act 2017* (au).

Beach, D. (2017). Process-Tracing Methods in Social Science. *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.176

Bennett, C. J. (1992a). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press.

Bennett, C. J. (2008). Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States. *Governance*, *1*, 415–441. https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-0491.1988.tb00073.x

Bennett, C. J., & Raab, C. D. (2017). *The Governance of Privacy: Policy Instruments in Global Perspective*. Routledge.

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Review*, *24*(6), 508–520. https://doi.org/10.1016/j.clsr.2008.09.001

Blatter, J., & Haverland, M. (2012). *Designing Case Studies: Explanatory Approaches in Small-N Research*. Palgrave Macmillan.

Börzel, T. A. (2002). Member State Responses to Europeanization. *JCMS: Journal of Common Market Studies*, *40*(2), 193–214. https://doi.org/10.1111/1468-5965.00351

Börzel, T. A., & Risse, T. (2012). From Europeanisation to Diffusion: Introduction. *West European Politics*, *35*(1), 1–19. https://doi.org/10.1080/01402382.2012.631310

Börzel, T., & Risse, T. (2002). *When Europe Hits Home: Europeanization and Domestic Change* (SSRN Scholarly Paper ID 302768). Social Science Research Network. https://doi.org/10.2139/ssrn.302768

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Bradford, A. (2015). Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, *42*, 158–173. https://doi.org/10.1016/j.irle.2014.09.004

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Branch, L. S. (2018, November 1). *Consolidated federal laws of canada, Breach of Security Safeguards Regulations*. https://laws-lois.justice.gc.ca/eng/regulations/SOR-2018-64/page-1.html

Branch, L. S. (2019, June 21). *Consolidated federal laws of canada, Personal Information Protection and Electronic Documents Act*. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

Buller, J., & Gamble, A. (2002). Conceptualising Europeanisation. *Public Policy and Administration*, *17*(2), 4–24. https://doi.org/10.1177/095207670201700202

Bürzel, T. A. (1999). Towards Convergence in Europe? Institutional Adaptation to Europeanization in Germany and Spain. *JCMS: Journal of Common Market Studies*, *37*(4), 573–596. https://doi.org/10.1111/1468-5965.00197

Busch, A. (2006). From Safe Harbour to the Rough Sea: Privacy Disputes across the Atlantic. *SCRIPTed: A Journal of Law, Technology and Society*, *3*(4), 304–321. https://heinonline.org/HOL/P?h=hein.journals/scripted3&i=311

Busch, P.-O., & Jörgens, H. (2011). The Diffusion of Renewable Energy Policies in Europe: Potentials and Pitfalls of an Alternative Europeanisation Mechanism. *European Energy Policy*, 97–123.

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law, 6*(2), 77–78. https://doi.org/10.1093/idpl/ipw006

Bygrave, Lee A. (2010). *Privacy and Data Protection in an International Perspective*. 36.

Bygrave, Lee Andrew. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

Campbell, R. (1989, November 2). Govt may be asked to alter Privacy Act. *Canberra Times (ACT: 1926 - 1995)*, 10. http://nla.gov.au/nla.news-article120857217

Canadian, Government. (n.d.). *Strengthening Privacy for the Digital Age—Innovation for a Better Canada* [Landing Pages]. Innovation, Science and Economic Development Canada. Retrieved 20 April 2020, from https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

Cantero Gamito, M. (2018). Europeanization through Standardization: ICT and Telecommunications. *Yearbook of European Law*, *37*, 395–423. https://doi.org/10.1093/yel/yey018

Collier, D. (2011). Understanding Process Tracing. *PS: Political Science & Politics*, *44*(04), 823–830. https://doi.org/10.1017/S1049096511001429

Collier, D., Brady, H. E., & Seawright, J. (2010). Outdated Views of Qualitative Methods: Time to Move On. *Political Analysis*, *18*(4), 506–513. https://doi.org/10.1093/pan/mpq022

Complaints against Globe24h.com, No. 2015–002 (Privacy Commissioner of Canada 5 June 2015). http://canlii.ca/t/gjk0b

Cowles, M. G., Risse, T., & Caporaso, J. (2001). *Transforming Europe: Europeanization and Domestic Change*. Cornell University Press.

Dimitrova, A., & Dragneva, R. (2009). Constraining external governance: Interdependence with Russia and the CIS as limits to the EU's rule transfer in the Ukraine. *Journal of European Public Policy*, *16*(6), 853–872. https://doi.org/10.1080/13501760903087894

Drezner, D. W. (2008). *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton University Press.

EU Comission. (2020). *Total services, detailed geographical breakdown by EU Member States (since 2010) (BPM6)—Eurostat*. EuroStat. https://ec.europa.eu/eurostat/web/products-datasets/-/bop_its6_tot

EUR-Lex—12002E/TXT - EN. (n.d.). [Text/html; charset=UTF-8]. Official Journal C 325 , 24/12/2002 P. 0033 - 0184; Official Journal C 340 , 10/11/1997 P. 0173 - Consolidated Version; OPOCE. Retrieved 12 May 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12002E/TXT&from=EN

EUR-Lex—31981H0679—EN. (n.d.). [Text/html; charset=UNICODE-1-1-UTF-8]. Official Journal L 246 , 29/08/1981 P. 0031 - 0031; Spanish Special Edition: Chapter 16 Volume 1 P. 0077; Portuguese Special Edition Chapter 16 Volume 1 P. 0077; Retrieved 25 February 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31981H0679&from=EN

EUR-Lex—31995L0046—EN. (n.d.). [Text/html; charset=UTF-8]. Official Journal L 281 , 23/11/1995 P. 0031 - 0050; Retrieved 25 February 2020, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Falkner, G., Treib, O., Hartlapp, C. for G. and O. S. M., Hartlapp, M., & Leiber, S. (2005). *Complying with Europe: EU Harmonisation and Soft Law in the Member States*. Cambridge University Press.

Farrell, H. (2003). Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/S0020818303572022

Flockhart, T. (2010). Europeanization or EU-ization? The Transfer of European Norms across Time and Space. *JCMS: Journal of Common Market Studies*, *48*(4), 787–810. https://doi.org/10.1111/j.1468-5965.2010.02074.x

Fromhol, J. (2000). THE EUROPEAN UNION DATA PRIVACY. *Berkley Technology Law Journal*, *15*, 461–484.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

González Fuster, G., & Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review*, *29*(5), 531–539. https://doi.org/10.1016/j.clsr.2013.07.008

Government of Canada, D. of J. (2017, February 10). *Proposed Legislation—Canada's Sytem of Justice*. https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html

Grabbe, H. (n.d.). *A Partnership for Accession? The Implications of EU Conditionality for the Central and East European Applicants*. 35.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Gregou, M. (2019). Conditionality, migration control and bilateral disputes: The view from the Greek–Turkish borders in the Aegean. *Mediterranean Politics*, *24*(1), 84–105. https://doi.org/10.1080/13629395.2017.1380117

Gschwend, T., & Schimmelfennig, F. (2007). Introduction: Designing Research in Political Science — A Dialogue between Theory and Data. In T. Gschwend & F. Schimmelfennig (Eds.), *Research Design in Political Science* (pp. 1–18). Palgrave Macmillan UK. https://doi.org/10.1057/9780230598881_1

Gschwend, T., & Schimmelfennig, F. (2011). *Research design in political science: How to practice what they preach*. Palgrave Macmillan. http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9780230598881

Hüllen, V. V. (2012). Europeanisation through Cooperation? EU Democracy Promotion in Morocco and Tunisia. *West European Politics*, *35*(1), 117–134. https://doi.org/10.1080/01402382.2012.631317

Information Commissioner UK. (2019, October 28). *Blog: GDPR is an evolution in data protection, not a burdensome revolution*. https://ico.org.uk/about-the-ico/news-and-events/blog-gdpr-is-an-evolution-in-data-protection-not-a-burdensome-revolution/

Jacquot, S., & Woll, C. (2003). *Usage of European Integration—Europeanisation from a Sociological Perspective*. *7*(12), 1–18.

James, S. (2007). *Europeanisation as 'Projection': Understanding the Changing Face of EU Policy Making within the Core Executive*. *2*, 30.

Jörgens, H. (2004). Governance by Diffusion: Implementing Global Norms through Cross-National Imitation and Learning. In W. Lafferty, *Governance for Sustainable Development* (p. 3367). Edward Elgar Publishing. https://doi.org/10.4337/9781845421700.00017

Kampen, J., & Swyngedouw, M. (n.d.). The Ordinal Controversy Revisited. *Quality and Quantity*, *34*, 87–102. Retrieved 14 April 2020, from https://link.springer.com/article/10.1023/A:1004785723554

Kirby, M. (2011). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law*, *1*(1), 6–14. https://doi.org/10.1093/idpl/ipq002

Klüche, M. (n.d.). The extraterritorial effect of EU food regulations on New Zealand – the example of wine. *Wageningen University*, 116.

Knill, C., & Lenschow, A. (1998). Coping with Europe: The impact of British and German administrations on the implementation of EU environmental policy. *Journal of European Public Policy*, *5*(4), 595–614. https://doi.org/10.1080/13501769880000041

Kremenyuk, V. A. (1988). The Emerging System of International Negotiations Columns. *Negotiation Journal*, *4*(3), 211–220. https://heinonline.org/HOL/P?h=hein.journals/nejo4&i=210

Krippendorff, K. (n.d.). *Content Analysis*. 8.

Lavenex, S. (2004). EU external governance in 'wider Europe'. *Journal of EUropean Public Policy*, *11*(4), 680–700. https://doi.org/10.1080/1350176042000248098

Lazer, D. (2001). Regulatory interdependence and international governance. *Journal of European Public Policy*, *8*(3), 474–492. https://doi.org/10.1080/13501760110056077

Levi-Faur, D. (2010). REGULATION & REGULATORY GOVERNANCE. *Jerusalem Papers in Regulation and Governance*, *1*, 48.

Liefferink, D. (2003). The Europeanisation of National Administrations. Patterns of Institutional Change and Persistence. *Acta Politica*, *38*(3), 279–282. https://doi.org/10.1057/palgrave.ap.5500020

Lynskey, O. (2017). The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, *19*, 252–286. https://doi.org/10.1017/cel.2016.15

Manners, I. (2002). Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies*, *40*, 235–258. https://doi.org/10.1111/1468-5965.00353

Mastenbroek, E., & Kaeding, M. (2006). Europeanization Beyond the Goodness of Fit: Domestic Politics in the Forefront. *Comparative European Politics*, *4*(4), 331–354. https://doi.org/10.1057/palgrave.cep.6110078

Mcclennan, J., & Schick, V. (n.d.). *"O, PRIVACY" CANADA'S IMPORTANCE IN THE DEVELOPMENT OF THE INTERNATIONAL DATA PRIVACY REGIME*. *38*, 25.

Mckenzie, L., & Meissner, K. L. (2017). Human Rights Conditionality in European Union Trade Negotiations: The Case of the EU–Singapore FTA. *JCMS: Journal of Common Market Studies*, *55*(4), 832–849. https://doi.org/10.1111/jcms.12522

Meunier, S., & McNamara, K. R. (2007). *Making History: European Integration and Institutional Change at Fifty*. Oxford University Press.

Nicolaides, P. A. (2010). A Model of Europeanisation with and without Convergence. *Intereconomics*, *2010*(2), 114–121. https://www.intereconomics.eu/contents/year/2010/number/2/article/a-model-of-europeanisation-with-and-without-convergence.html

Nogueras, D. J. L., & Martinez, L. M. H. (2001). Human Rights Conditionality in the External Trade of the European Union: Legal and Legitimacy Problems. *Columbia Journal of European Law*, *7*(3), 307–336. https://heinonline.org/HOL/P?h=hein.journals/coljeul7&i=313

Noutcheva, G., & Aydin-Düzgit, S. (2012). Lost in Europeanisation: The Western Balkans and Turkey. *West European Politics*, *35*(1), 59–78. https://doi.org/10.1080/01402382.2012.631313

OAIC. (2020). *History of the Privacy Act*. OAIC. https://www.oaic.gov.au/privacy/the-privacy-act/history-of-the-privacy-act/

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data—OECD*. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD DATA. (2020). *GDP and spending—Gross domestic product (GDP)—OECD Data*. TheOECD. http://data.oecd.org/gdp/gross-domestic-product-gdp.htm

Office of the Canadian Privacy Commissioner. (2004, April 1). *How PIPEDA applies to charitable and non-profit organizations*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/

Office of the Canadian Privacy Commissioner. (2006, July 19). *Commissioner's Findings - PIPEDA Case Summary #2006-333: Canadian-based company shares customer personal information with*

U.S. parent. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-333/

Office of the Canadian Privacy Commissioner. (2009, January 27). *Guidelines for processing personal data across borders*. https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

Office of the Canadian Privacy Commissioner. (2018, October 29). *What you need to know about mandatory reporting of breaches of security safeguards*. https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Office of the Canadian Privacy Commissioner *411Numbers ceases practice of removing information for a fee*, No. 2019–005 (25 March 2019). http://canlii.ca/t/j3wmk

Onuch, O. (2015). EuroMaidan Protests in Ukraine: Social Media Versus Social Networks. *Problems of Post-Communism*, *62*(4), 217–235. https://doi.org/10.1080/10758216.2015.1037676

Orbie, J. (2006). Civilian power Europe: Review of the original and current debates. *Cooperation and Conflict*, *41*(1), 123–128.

Orbie, J., & Carbone, M. (2016). The Europeanisation of development policy. *European Politics and Society*, *17*(1), 1–11. https://doi.org/10.1080/23745118.2015.1082688

Peltz-Steele, R. J. (2015). *The Pond Betwixt: Differences in the U.S.-EU Data Protection/Safe Harbor Negotiation*. 19.

Perkins, R., & Neumayer, E. (2004). Europeanisation and the Uneven Convergence of Environmental Policy: Explaining the Geography of EMAS. *Environment and Planning C: Government and Policy*, *22*(6), 881–897. https://doi.org/10.1068/c0404j

Platsas, A. (2008). The Functional and the Dysfunctional in the Comparative Method of Law: Some Critical Remarks. *Electronic Journal of Comparative Law*, *12*(3).

Princen, S. (2003). Exporting regulatory standards. Understanding the European Union's External Relations 29 (2003): 140. In *Understanding the European Union's External Relations* (pp. 140–154). Routledge.

Radaelli, C. M. (2004). The Puzzle of Regulatory Competition. *Journal of Public Policy*, *24*(1), 1–23. https://doi.org/10.1017/S0143814X04000017

Salbu, S. R. (2002). The European Union Data Privacy Directive and International Relations. *Vanderbilt Journal of Transnational Law*, *2*, 655–696. https://heinonline.org/HOL/P?h=hein.journals/vantl35&i=670

Samuelson, P., Schwartz, P. M., Reidenberg, J. R., Swire, P. P., & Litan, R. E. (1999). A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy. *California Law Review*, *87*(3), 751. https://doi.org/10.2307/3481032

Schimmelfennig, F. (2010). Europeanisation Beyond the Member States. *Zeitschrift Für Staats- Und Europawissenschaften (ZSE) / Journal for Comparative Government and European Policy*, *8*(3), 319–339. JSTOR. https://www.jstor.org/stable/24237074

Schimmelfennig, F., & Sedelmeier, U. (2004). Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe. *Journal of European Public Policy*, *11*(4), 661–679. https://doi.org/10.1080/1350176042000248089

Schünemann, W. J., & Windwehr, J. (2017). *Supranational norm entrepreneurship or uploading of high standards: The case of the European data protection regulation and the role of the European Parliament*. 18.

Sinopoli, D., & Purnhagen, K. (2016). REVERSED HARMONIZATION OR HORIZONTALIZATION OF EU STANDARDS?: *Wisconsin International Law Journal*, *34*(1), 28.

Smith, K. (1998). The use of political conditionality in the EU's relations with third countries: How effective? *European Foreign Affairs Review*, *3*(2), 253–274.

Smith, M. (1996). The European Union and a Changing Europe: Establishing the Boundaries of Order. *JCMS: Journal of Common Market Studies*, *34*, 5–28. https://doi.org/10.1111/j.1468-5965.1996.tb00558.x

Smith, M. L. (2010). Testable Theory Development for Small-N Studies: Critical Realism and Middle-Range Theory. *International Journal of Information Technologies and Systems Approach*, *3*(1), 41–56. https://doi.org/10.4018/jitsa.2010100203

Spohn, W., & Triandafyllidou, A. (Eds.). (2003). *Europeanisation, National Identities and Migration: Changes in Boundary Constructions between Western and Eastern Europe* (1st ed.). Routledge. https://doi.org/10.4324/9780203217511

Tan, D. R. (n.d.). *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union*. *21*, 25.

Taylor, M. (1989, January 19). Privacy rules 'more onerous' for PS. *Canberra Times (ACT: 1926 - 1995)*, 3. http://nla.gov.au/nla.news-article120905128

Terwangne, C. de. (2014). The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data. *International Review of Law, Computers & Technology*, *28*(2), 118–130. https://doi.org/10.1080/13600869.2013.801588

Trachtman, J. P. (1993). International Regulatory Competition, Externalization, and Jurisdiction. *Harvard International Law Journal*, *34*(1), 47–104. https://heinonline.org/HOL/P?h=hein.journals/hilj34&i=53

Trondal, J. (2005). Two Worlds of Europeanisation – Unpacking Models of Government Innovation and Transgovernmental Imitation. *European Integration Online Papers*, *9*(1). http://eiop.or.at/eiop/texte/2005-001a.htm

UNCTAD | Data Protection and Privacy Legislation Worldwide. (2020). https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Vogel, D. (2009). *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Harvard University Press.

Westin, A. (1967). *Privacy and Freedom*. Atheneum.

Wickens, M. R. (1972). A Note on the Use of Proxy Variables. *Econometrica*, *40*(4), 759–761. JSTOR. https://doi.org/10.2307/1912971

World Bank. (2020). *Digital Adoption Index* [Text/HTML]. World Bank. https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index