Legalization of Privacy and Personal Data Governance: Feasibility Assessment for a New Global Framework Development

Ravinder Singh

Thesis submitted to the Faculty of Graduate and Postdoctoral Studies in partial fulfillment of the requirements for the Doctor of Laws (LL.D.) degree

Common Law Section
Faculty of Law
University of Ottawa

"To Mother Nature"

Acknowledgments

I am very thankful to Prof. Michael Geist, my thesis supervisor, for his exceptional supervision and guidance. I am also grateful to Prof. Kevin McMillan, the thesis co-supervisor, for his excellent reviews and critical feedback. Moreover, I would like to thank the members of the thesis examination committee—Teresa Scassa, Ian Kerr, Patrick Leblond, and Avner Levin—for helping me to improve the thesis with their constructive feedbacks. I am also grateful to the University of Ottawa and the Social Sciences and Humanities Research Council for financial support. Finally, I am also thankful to my friends and family for their unconditional support.

Legalization of Privacy and Personal Data Governance: Feasibility Assessment for a New Global Framework Development

Ravinder Singh
Doctor of Laws (LL.D.)
Faculty of Law, University of Ottawa

Abstract

The International Conference of Data Protection and Privacy Commissioners has been actively engaged in the development of a new, legally binding international framework for privacy and data protection. Given the existence of three international privacy and data protection regimes (i.e. the OECD Privacy Guidelines, the EU data protection framework and the APEC Privacy Framework) and the availability of other bilateral venues to resolve transnational data flows issues (e.g. the EU-US Safe Harbor agreement, the Umbrella Agreement and the latest, the Privacy Shield arrangement), the thesis asks whether the development of such a new regime is feasible.

The main finding of the thesis is that in an era of a globalized society driven by the internet and information-communications technology, where all three of the leading international privacy and data protection regimes are consistently updating and modifying their respective frameworks, and where there is persistent divergence between the European Union and the United States approaches towards transborder data flow, the emergence of a new, legally binding international framework is unlikely, at least under the prevailing circumstances.

Therefore, the thesis calls for a shift towards an institutionalized arrangement that is founded on existing international co-operation and convergence and that further expands ongoing inter-regime collaboration. The approach recommended in the thesis is an effective alternative to the development of a new, legally binding international framework, and even offers strong prospects for the evolution of a legalized arrangement for international privacy and personal data governance in due course.

Table of Contents

Table of Abbreviations

ACTA	Anti-Counterfeiting Trade Agreement
APEC	Asia Pacific Economic Co-operation
APPA	Asia Pacific Privacy Authorities
CBPR	Cross-Border Privacy Rules
CDD	Centre for Digital Democracy
COE	Convention of Europe
CPEA	Cross-Border Privacy Enforcement Arrangement
DOC	Department of Commerce
DPA	Data Protection Authorities
EC	European Commission
ECHR	European Court of Human Rights
ECJ	European Court of Justice
ECPHRFF	European Convention for the Protection of Human Rights and Fundamental Freedoms
EPIC	Electronic Privacy Information Centre
EU	European Union
FTA	Free Trade Agreement
FTC	Federal Trade Commission
GCIG	Global Commission on the Internet Governance
GDPR	General Data Protection Regulation
GPEN	Global Privacy Enforcement Network
ICC	International Chamber of Commerce
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICESCR	International Covenant on Economic, Social and Cultural Rights
ILC	International Law Commission
ISO	International Organization for Standardization
NGO	Non-Governmental Organization
NSA	Non-State Actors
OECD	Organization for Economic Cooperation and Development

PEA	Privacy Enforcement Authorities
PNR	Passenger Name Records
SSHRC	Social Sciences and Humanities Research Council of Canada
SSRN	Social Science Research Network
TBDF	Transborder Data Flows
TRIPS	Trade-Related Aspects of Intellectual Property Rights
TTIP	Transatlantic Trade and Investment Partnership
UDHR	Universal Declaration of Human Rights
UN	United Nations
US	United States
USNSA	United States National Security Agency
WIPO	World Intellectual Property Organization
WP	Working Party
WPISP	Working Party on Information Security and Privacy
WTO	World Trade Organization

Chapter I. Introduction

1. The argument—research question and research outcomes

This thesis explores whether the development of a new global regime or framework[1] for privacy and data protection[2] is feasible.[3] The rationale for this feasibility assessment lies in the observation that 1) the existing divergence among national and international privacy and data

[1] Hereinafter, the terms international frameworks or regimes have been used interchangeably to convey a general reference to privacy and data protection governance, which generally includes laws, regulations, guidelines, practices, codes, and other policy instruments. Further, Colin J. Bennett (Bennett) has recognized such conceptual complexity by listing an inventory of policy instruments—national legislation, international agreements, self-regulatory mechanisms (codes, seals and standards), privacy impact assessments, and privacy-enhancing technologies. See Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008)" at xi [Bennett, "Privacy Advocates"]. Moreover, these terms are used in a generic sense unless qualified by a specific reference; for example, the Organization for Economic Co-operation and Development (OECD) regime encompasses the Privacy Guidelines of 1981 (OECD Privacy Guidelines) and the Revised Privacy Guidelines of 2013 (Revised Privacy Guidelines), the European Union (EU) framework involves both the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 108 (COE 108) and EU Data Directive 95/46/EC (Data Directive 95/46/EC) and the Asia-Pacific Economic Co-operation (APEC) regime involves Privacy Framework, 2004 (APEC Privacy Framework).

[2] Hereinafter, the term "privacy and data protection" has been used interchangeably with terms such as "privacy and personal data", "personal data and privacy", "data protection and privacy", "data protection", and "privacy" in order to encompass the variety of references in the academic literature and policy realm. Despite that flexibility, these terms enshrine a concept of privacy in a personal data context generally described as "information privacy" or "personal data protection" from the European perspective. For an interesting take on the concept of privacy and data protection from both the EU and US perspectives, see Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects" (2009) 25.4 Computer Law and Security Review 307 [Kuner, "International Legal Framework"] (asserting that "[t]here are also differences in the way these terms are understood in different legal systems and regions" at 309); Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford, UK: Oxford University Press, 2014) [Bygrave, "International Perspective"] (describing data privacy law as "specifically regulat[ing] all or most stages in the processing of certain kinds of data" at 1); see Chapter II's discussion of the conceptualization of privacy and data protection.

[3] The notion of feasibility is specified in terms of the evolution of a legally binding international framework on privacy and data protection as pursued by the Commissioners' Conference. According to the Merriam-Webster dictionary the term "feasible" means "capable of being done or carried out". See online: merriam-webster <http://www.merriam-webster.com/dictionary/feasible>. In operational terms, an assessment of the feasibility of developing a new regime in the present context explores whether the Commissioners' Conference would be able to develop an international consensus behind the development of a new, legally binding international framework.

protection measures 2) along with adverse implications of the advancements in internet and information communication technology (ICT) and 3) the expanding role of personal data in an evolving global information society has made it harder to cope with the emerging challenges.[4] Despite the emergence of a significant convergence amongst various international privacy and data protection regimes on common objectives and a principles-based approach,[5] the emerging trends indicate an alarming diminution and deterioration in privacy and personal data protection, whether that relates to cyberspace or state surveillance activities. One such trend is illustrated by the ongoing revelations by Edward Snowden (Snowden) about the unprecedented reach of the United States (US) National Security Agency's (USNSA) surveillance program.[6] As a consequence, various national and international measures[7] have been launched to address

[4] See Marc Rotenberg, "Preserving Privacy in the Information Society", online: unesco.org <http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm> ("The threats to privacy came from multiple sources. They can be broadly classified as technological threats, threats from actions of government, and threats from the private sector and commercial services"); see also Philip E. Agre and Marc Rotenberg, eds, *Technology and Privacy: The New Landscape* (Cambridge Mass: MIT Press, 1997); Fred H. Cate, *Privacy in the Information Age* (Washington, DC: Brookings Institution Press, 1997) [Cate, "Privacy Information Age"]; Bruce Phillips, "Privacy in the Information Age: an Oxymoron?" (26 January 1995), online: OPC Archived Speeches <https://www.priv.gc.ca/media/spd/archive/02_05_a_950126_e.asp> ("The [privacy] law seems particularly ill-suited to address the many issues flowing from many new information technologies…").

[5] For further discussion of this convergence, see Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Massachusetts: MIT Press, 2006) [Bennett & Raab, "Governance of Privacy"] ("We demonstrate how laws have increasingly converged around a common set of substantive and procedural principles…") at xxv; Colin J. Bennett, "Review Article: What is Policy Convergence and What Causes it?" (1991) 21:2 British Journal of Political Science 215; ———"Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States" (1988) 1:4 Governance 415.

[6] Edward Snowden's revelations about the massive breadth of the US National Security Agency's (US-NSA) surveillance program created worldwide tumult and forced various countries around the world to update their national data privacy legal frameworks and to enhance data security technological capacities. See Wikipedia webpage on Edward Snowden, online: Wikipedia: Edward Snowden <https://en.wikipedia.org/wiki/Edward_Snowden> [Snowden, "Wikipedia"]. For international reaction to Snowden's revelations, see also Wikipedia webpage, online: Wikipedia, Reactions to Global Surveillance Disclosures <https://en.wikipedia.org/wiki/Reactions_to_global_surveillance_disclosures>.

[7] E.g. in 2012 the EU launched its data protection overhaul drive with the General Data Protection Regulation (GDPR) initiative in order to harmonize and update data protection rules throughout the EU. See European Commission, "Commission Proposes a Comprehensive Reform of the Data Protection Rules" (25 January 2012), online: European Commission

some of the emerging challenges[8] to privacy and data protection. However, a credible state-led international initiative towards the development of a new global framework is yet to emerge. The International Conference of Data Protection and Privacy Commissioners (Commissioners' Conference)[9] along with other non-state stakeholders[10] have long demanded the development of a new, legally binding international framework.[11] The Commissioners' Conference has taken several steps towards the fulfillment of that objective including a demand for a United Nations (UN) convention. This thesis investigates whether the development of a new, legally binding international regime is feasible.

<http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> [EU, "Proposed Reforms"]; similarly, the US introduced in February 2012 the *Consumer Privacy Bill of Rights*; see The White House, "We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online" (23 February 2012), online: White House <https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>. For additional information on ongoing US measures, see the Electronic Privacy Information Centre (EPIC), "White House: Consumer Privacy Bill of Rights", online: EPIC <https://epic.org/privacy/white_house_consumer_privacy_.html>.

[8] In this thesis, the phrase 'emerging challenges' will typically be used to refer to the international aspects of new problems of privacy and personal data governance that have arisen in the context of expanding transborder data flows and an increasingly globalised information society. For example, Snowden's revelations brought to light one of the major new challenges facing existing national and international legal privacy and data protection regimes: the problem of the immense reach of the NSA's global surveillance program. A more recent example that highlights another aspect of emerging challenges to privacy and data protection in transborder data flows is the recent European Court of Justice or Court of Justice of the European Union (ECJ) *Schrems* decision, which invalidates the EU-US Safe Harbor framework. See *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14); Case online: Infocuria <http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=328696> [*Schrems* decision]. See also Chapter III for an extended discussion of the nature, scope and implications of these emerging challenges.

[9] The annual gathering of the privacy enforcement authorities (PEA) or data protection authorities (DPA) at the International Conference of Data Protection and Privacy Commissioners (Commissioners' Conference) has emerged one of the major international platforms pushing for the development of a new, legally binding international framework for privacy and data protection. For a detailed discussion of the Commissioners' Conference initiatives, see Chapter III, below.

[10] E.g. EPIC has raised this demand from time to time at various US Congress hearings and other international platforms. For additional information on EPIC's engagement; online: EPIC <https://epic.org>.

[11] See for additional information on the Commissioners' Conference's efforts towards a new, legally binding international framework, Chapter II, below.

The main finding of the thesis is that a new, legally binding global framework on privacy and data protection is unlikely to emerge, at least in the near future. On the one hand, the existing international privacy and data protection regimes[12] have launched various initiatives for an enhanced co-operation and collaboration to address the emerging challenges whereas on the other hand, two of the world's leading economies and major stakeholders in privacy and data protection—the US and the European Union (EU)—have been able to resolve transnational disputes over transborder data flows through bilateral agreements, like the Safe Harbor agreement[13] or the recently concluded the Umbrella Agreement[14] and the Privacy Shield arrangement.[15] Despite these positive developments, however, divergence between the three regimes persists, particularly over enforcement measures and the significantly different general approaches adopted by the US and EU. This divergence has made it hard to reach the kind of

[12] The three international privacy and data protection regimes are: the OECD Privacy Guidelines (1980, 2013), the EU data protection framework, which includes the COE 108 and Data Directive 95/46/EC and the APEC Privacy Framework, 2004.

[13] See the US Department of Commerce (DOC), the EU-US Safe Harbor framework documents, online: export.gov <http://www.export.gov/safeharbor/> [Safe Harbor agreement].

[14] See European Commission, Press Release Database, "Questions and Answers on the EU-US Data Protection 'Umbrella Agreement'" (8 September 2015), online: European Commission <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>; a detailed draft of the Umbrella Agreement, released by the EU Parliament, see online: European Commission <http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf> [Draft Umbrella Agreement]; see also EPIC, "EU-US Umbrella Agreement", online: EPIC <https://epic.org/privacy/intl/data-agreement/>; Douwe Korff, "EU-US Umbrella Data Protection Agreement: Detailed Analysis" (14 October 2015), online: European Area of Freedom Security & Justice <http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/>.

[15] On February 29, 2016 the European Commission released the details on the EU-US Privacy Shield. For detailed information on the EU-US Privacy Shield, see European Commission, "European Commission Unveils EU-U.S. Privacy Shield" (29 February 2016), online: European Commission ""<http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm> [EU-US Privacy Shield]; see also, the European Commission's adequacy decision on the proposed EU-US Privacy Shield, online: European Commission <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf> [Adequacy of the EU-US Privacy Shield]; Martin A. Weiss & Kristin Archick, "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield" (12 February 2016), online: US Congress Research Services <https://www.fas.org/sgp/crs/misc/R44257.pdf>; EPIC, "Privacy Shield EU-U.S. Data Transfer Arrangement", online: <https://www.epic.org/privacy/intl/privacy-shield/>.

international consensus needed to launch a concerted, state-led initiative to develop a new, legally binding international framework.

The thesis recommends a re-orientation of the focus of ongoing international efforts, including those of the Commissioners' Conference, away from hard legalization, and towards exploring other, soft-legalization solutions and strategies. The thesis suggests that we should work on strategies for institutionalizing the co-operation of the existing international privacy and data protection regimes. These strategies should draw on multiple resources, including the expertise of the privacy enforcement authorities and existing forms of inter-regime collaboration. They must also take into consideration the national interests of the major states involved, interests that come to light when the pattern of confrontations between the US and EU is examined. The concluding chapter argues for institutionalization strategies of this sort, aimed at further enhancing existing forms of collaboration between the three major regimes. The following discussion first introduces the thesis' main research question and its analytical components, then briefly reflects on some of the underlying premises and ends with a summary of the ultimate conclusions of the thesis and a presentation of its recommended alternative.

How to address the emerging challenges to privacy and data protection? Does the development of a new, legally binding international framework, as pursued by the Commissioners' Conference, offer the most constructive alternative? Why are the ongoing efforts of the international regimes not sufficient? What about the strategies pursued by the world's leading economies and stakeholders in privacy and data protection, the US and the EU, to resolve transnational issues over transborder data flows, wherever they emerge? Given the complexity of the evolving pattern of privacy and personal data governance, what are the likely prospects for the emergence of a new, legally binding international framework? These questions animate the rationale of this research project. To ensure a focused and systematic investigation, the thesis poses the following overarching research question:

> *Given existing international conditions, is the development of a new, legally binding international framework on privacy and data protection feasible?*

This research question is addressed through an analytical research design that knits together three distinct analytical components when conducting this feasibility assessment. Although the central focus of the thesis is a critical examination of the Commissioners' Conference's

ongoing efforts at developing a new, legally binding international framework, any effective assessment of these efforts will require consideration of the three existing international regimes for privacy and data protection, as well as the ongoing history of bilateral confrontations between the US and the EU over privacy and data protection issues. The thesis pays special attention to the evolving forms of cooperation between the three international regimes, namely: the Organization for Economic Co-operation and Development (OECD) privacy governance regime that involves both the Privacy Guidelines of 1981[16] and the Revised Privacy Guidelines of 2013[17] (OECD Privacy Guidelines); the EU data protection framework that includes the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 108 (COE 108)[18] and the EU Data Directive 95/46/EC (Data Directive 95/46/EC)[19]; and the Asia-Pacific Economic Co-operation (APEC) Privacy Framework of 2004 (APEC Privacy Framework).[20] In the US-EU confrontations context, the main focus is on the Safe Harbor agreement; however, the recent European Court of Justice (ECJ) *Schrems* decision has invalidated the Safe Harbor agreement and resulted in the recently concluded EU-US Privacy Shield arrangement that builds on the Safe Harbor agreement, which is not implemented yet.[21]

To answer the research question, therefore, the thesis explores three major considerations. First, it takes stock of the increasing role of the data protection authorities (DPA), or the

[16] See OECD Privacy Guidelines, online: OECD <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [OECD Privacy Guidelines].

[17] See OECD Revised Privacy Guidelines, online: OECD <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [Revised Privacy Guidelines].

[18] See COE 108, online: COE <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> [COE 108].

[19] See EU Data Directive 95/46/EC, online: EUR-Lex <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en> [EU Data Directive 95/46/EC].

[20] See APEC Privacy Framework, online: APEC <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> [APEC Privacy Framework].

[21] See *Schrems* decision, *supra* note 8.

privacy enforcement authorities (PEA)[22], both in national and international privacy and personal data governance, with a particular emphasis on their efforts towards development of a new, legally binding international framework. Second, it explores the role of the three leading international regimes on privacy and personal data governance, again with a specific focus on international data flows. Third, it takes into account the role of national interests as manifested in the context of EU-US confrontations over transborder data flows. These three considerations—or what we have called 'analytical components'—in turn represent three different conceivable strategies for addressing international privacy and data protection issues: namely, 1) developing a new, legally binding international framework; 2) expanding on the ongoing efforts of the three international regimes to enhance their mutual coordination, interoperability and harmonization; and 3) maintaining the *status quo*, where, in addition to relying on existing national, regional and international agreements, states can protect their respective national interests by resolving privacy and data protection issues through bilateral agreements, as illustrated by the US-EU Safe Harbor agreement. These are the three main venues currently on offer for treating privacy and data protection at the international level. At the current juncture, the data protection authorities are vying for an enhanced role in privacy and personal data governance; the three existing international regimes seem to be in constant regime-overhaul mode; and major states are fighting hard to protect their national interests without unduly compromising their sovereignty.[23] On the one side, there are the Commissioners' Conference efforts towards development of a new, legally binding international regime, whereas, on the other side, there are the ongoing coordination efforts between the three international regimes, as well as ongoing confrontations between the major state actors. By synthesizing the analysis of these three considerations, the thesis explores various alternative strategies, including development of a new, legally binding regime proposition and possible alternatives to this strategy.

[22] Both phrases—the "data protection authorities" (DPA) and the "privacy enfacement authorities" (PEA)—are used interchangeably. Generally, "DPA" is prevalent in the EU while in other contexts, like APEC or the OECD, the term "privacy enforcement authorities" is widespread. For additional information on the notion of data protection authorities see Chapter IV, below.

[23] E.g. the US position in transnational confrontations over transborder data flows with the EU illustrates such posturing. This is one of the central arguments of the thesis, further developed in Chapter V and VI.

Also, it is important to briefly reflect on some of the principal assumptions undergirding the overall research design of this thesis. In principle, the demand for a new international regime, and ensuing efforts to create one, may emerge from any number of sites. However, recent trends in this age of global governance have seen non-state stakeholders emerge as strong contenders for this role, traditionally dominated by states. Nonetheless, it is still the case today that concerted efforts to construct a new international regime are widely seen to be the sovereign prerogative of states, particularly the leading powers. Although the role of the state remains central in any venture to develop a new international regime, it is no longer the only important actor in a global governance context, where multiple horizontal and vertical networks and arenas can flourish and participate in governance alongside states.[24] In recent years, the Commissioners' Conference has been engaged in various privacy and personal data governance activities. Its prevailing assumption has been that 'hard legalization' of governance in this sphere is necessary if emerging challenges are to be addressed effectively. However, for the most part, any hard legalization initiatives still remain the prerogative of sovereign states. The world's leading states, moreover, have already established the three international privacy and data protection regimes, and so far have preferred to address their transnational disputes over transborder data flows through bilateral agreements.

The guiding premise of the existing international privacy and data protection regimes is that they constitute the foundational infrastructure of international privacy and personal data governance and require special consideration when it comes to the question of developing any new regime. Whosoever — state or non-state actor — hopes to pursue the creation of a new regime will be bound to address existing regimes in that issue-area. This will be the case whether the hope is to build on the existing regime(s), to reform/overhaul the existing regime(s), or to replace the existing regime(s) entirely. Moreover, to be successful, any efforts to develop a new international framework in an issue-area in which states have already devised

[24] This proposition draws on Anne-Marie Slaughter's (Slaughter) theoretical conception of a "new world order." Slaughter argues that in this new world order, the state is not the only actor in the international system, but is still one of the most important actors; that rather than disappearing, the state is disaggregating into its component institutions, each with unique identities and professional experiences; and that transnational networks of these governmental components exist within and alongside traditional international organisations. See Ann-Marie Slaughter, *A New World Order* (Princeton, NJ: Princeton University Press, 2004) at 18 [Slaughter, "A New World Order"].

strategies and reached agreements will have to take into serious consideration the dynamics of existing national interests. Therefore, it makes sense to understand, and to seek explanations of, states' national interests with respect to the issue at hand. In the context of transborder data flows, these national interests are perhaps on most vivid display in ongoing transnational confrontations between the major state actors involved.

This approach not only introduces the existing national and international frameworks to the debate but also reveals the states' interests that can inform and explain their preferences. Such insight into states' behavior is necessary before speculating on the prospects for the development of a new regime where some of those states are presumed to lead such a venture. If we can understand and develop credible explanations of US and EU national interests, as revealed in the study of their transborder data flows confrontations, then that knowledge can help in devising strategies for developing new instruments.[25] The overall utility of the analytical-components framework is that it can assist in ongoing efforts to develop a new regime, by helping to strike an optimum balance among competing interests, objectives and instruments. Moreover, from a broader theoretical perspective, the study of ongoing EU-US confrontations over transborder data flows also offers deeper insights into the nature of the implicated national interests, which is again of critical importance to understand the complexity of privacy and personal data governance. Chapter V further develops this argument through application of the theoretical perspective proposed here. The main conclusions reached on each of the framework's analytical components are as follows:

1) On the data protection authorities, the thesis emphasizes their role as one of the emerging stakeholders in international privacy and personal data governance. They are well positioned to exert influence in international and domestic policy arenas. From a national perspective, given their statutorily mandated roles and responsibilities, the data protection authorities have access to various legalization channels to influence national privacy and personal data frameworks.[26]

[25] This adverts to our third theoretical dimension, the need to address the question of states' interests, which is fundamental to any efforts to develop a new international regime. Chapter V further elaborates the theory and its manifestations in the context of US-EU confrontations over transborder data flows.

[26] See Charles D. Raab, "Networks for Regulation: Privacy Commissioners in a Changing World" (2011) 13:2 Journal of Comparative Policy Analysis 195-96 [Raab, "Networks for Regulation"] ("DPAs'… functions go beyond legal enforcement to embrace a variety of promotional and policy-

Some of these opportunities include the production of annual reports before national parliaments or other legislative bodies to draw attention to important issues and developments, or participation in legislative processes through ministerial recommendations and congressional hearings or through litigation.[27] Significantly, the data protection authorities possess the capacity to internationalize their domestic privacy and data protection framework,[28] although that capacity largely depends on the leeway formally conferred on them by the overarching statutory governance scheme.[29] In the international arena, the data protection authorities act as an alliance of the various national data protection authorities and engage with international privacy and data protection regimes, international organizations and other international policy arenas dealing with issues of privacy and personal data governance. The nature and scope of the role of the data protection authorities' alliances in overall privacy and personal data governance is largely determined by the goals and objectives of those alliances[30] Moreover, the existing international privacy and data protection regimes have shown strong support for the data protection authorities' alliances by recognizing their critical role in

---

influencing activities, and they engage in relationships with those using non-official or extra-legal instruments for the protection of information privacy and the limitation of surveillance") at 195-96.

[27] E.g. the Office of the Privacy Commissioner of Canada (OPC) is engaged in "providing legal and policy analyses and expertise to help guide Parliament's review of evolving legislation to ensure respect for individuals' right to privacy; responding to inquiries of Parliamentarians, individual Canadians and organizations seeking information and guidance and taking proactive steps to inform them of emerging privacy issues…" For extra information, see online: OPC, Mandate and Mission <https://www.priv.gc.ca/au-ans/mm_e.asp>.

[28] See e.g. the OPC has been very active in influencing international privacy governance through active participation in various international policy forums and international organizations' activities. For additional insights into the Canadian privacy commissioner's role, see OPC, "Canada's Role and Influence in the Global Privacy Arena" (3 June 2011), online: OPC Speeches <https://www.priv.gc.ca/media/sp-d/2011/sp-d_20110603_cb_e.asp> ("And we use our international influence to concrete ends", statement made by Chantal Bernier, then Assistant Privacy Commissioner of Canada, indicating that intent).

[29] The Office of the Privacy Commissioner of Canada is the best illustration in this regard: it is authorized to play an active role in public advocacy and in raising issue-awareness. The OPC is created under the governing statute, *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), see online: Justce Laws Website <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>.

[30] See Chapter III's discussion on of the Commissioners' Conference further elaborates that proposition.

international privacy and personal data governance.[31] In addition, their pragmatic policy knowledge and accumulated expertise and experience in relation to law enforcement and implementation measures have been among the assets that have helped the data protection authorities consolidate their position.

Apart from these generalizations, a closer analysis of the Commissioners' Conference reveals some of their key strengths and limitations, helping us to assess their role in privacy and personal data governance. In Chapter III, a survey of some of the resolutions adopted by the Commissioners' Conference allows two sets of conclusions to be drawn: the first takes stock of the Conference's strategies and initiatives directly related to privacy and personal data governance, and the second reflects on the Commissioners' Conference's evolutionary trajectory. Extrapolating from some of the most recently adopted resolutions, we observe a significant retrenchment of the Conference's efforts to pursue a new, legally binding international framework.[32] A second important observation highlights the Conference's renewed efforts to institutionalize itself, particularly in response to the rise of other, parallel networks of privacy enforcement authorities.[33] Most of the theoretical insights and arguments on the data protection authorities are developed in Chapter IV, where the data protection authorities are interpreted conceptually as transgovernmental networks and assessed for their

---

[31] See e.g. the OECD adopted resolution, "Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy", recommended the establishment of an informal network of privacy enforcement authorities, which resulted in the emergence of Global Privacy Enforcement Network (GPEN). It states (para. 21):

> Member countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.

See online: OECD <http://www.oecd.org/internet/ieconomy/38770483.pdf> [OECD Recommendation on Cross-border Co-operation].

[32] This argument is based on the analysis of some of the adopted resolutions of the data protection authorities, where the Commissioners' Conference appears to have increasingly focused on enhancing institutionalization. For details, see Chapter III analysis of the Commissioners' Conference's ongoing efforts.

[33] See e.g. the emergence of the GPEN at the behest of the OECD. See online: GPEN <https://www.privacyenforcement.net> [GPEN]. For additional details, see Chapter III and IV, below.

strengths and limitations in the light of global governance literature. A generalized theoretical framework is developed and applied to the Commissioners' Conference in order to draw conclusions based on an empirical account of their ongoing activities. Chapter IV concludes with observations along four dimensions: the data protection authorities' relationship with international privacy and data protection regimes, international organizations, national frameworks, and other alliances of privacy enforcement authorities; their efforts towards a new, legally binding international instrument; their institutionalization efforts; and the implications of the foregoing for the research question and for the thesis's findings.

2) The three international privacy and data protection regimes are the central fixtures of international privacy and personal data governance. With respect to the international regimes, Chapter III takes stock of the ongoing measures at all three international privacy regimes, whereas Chapter II offers a general overview of the existing international governance framework, and Chapter V presents a theoretical argument by drawing on the international legalization literature. The thesis recognizes the leading role of the three international regimes in national and international privacy and personal data governance. From a national perspective, the existing regimes are the site of first response for governance efforts, invoked as the main vehicles designed and deployed to address the emerging challenges. All three privacy and data protection regimes have thus launched a variety of initiatives. For example, the OECD updated the Privacy Guidelines (1981) with the Revised Privacy Guidelines in 2013, whereas the EU launched measures for the modernization of the COE 108 and the adoption of General Data Protection Regulation (GDPR).[34] In any case, the member states have mobilized the existing international privacy and data protection regimes to undertake comprehensive measures to respond to emerging challenges, in particular those posed by rapidly evolving internet and information communication technologies.

The international privacy and data protection regimes are the fundamental instruments of global privacy governance created through the cooperative efforts of states. Nonetheless, the thesis' interdisciplinary approach helps identifying the legalization literature of the international relations (IR) scholarship as a useful theoretical framework for analyzing this

[34] For additional details on the ongoing efforts at the international regimes' level, see Chapter III and its discussion of all three of the international privacy and data protection regimes.

issue. Thus, in Chapters IV and V the thesis utilizes legalization theory and conceptualizes the three regimes along the hard- vs. soft-law spectrum. Then, against the backdrop of the advantages and disadvantages of both hard- and soft-law forms, the relations among the three regimes are analyzed. One of the main objectives of the thesis is to understand and explore the role of the existing international privacy and data protection regimes not only in their individual capacities but also in terms of their collective role in the evolution of privacy and personal data governance.

As conceptualized along the hard- vs. soft-law spectrum, and its constituent components—obligation, precision and delegation—, the EU regime is ultimately categorized as a hard-law form oriented to strong enforcement measures, whereas the OECD Privacy Guidelines and the APEC Privacy Framework are identified as soft-law forms aiming for flexibility on enforcement and implementation measures. Once that conceptualization is established, theoretical implications are derived for the inter-relationship among the three privacy regimes. By applying Abbott & Snidal's and Shaffer & Pollack's theoretical approaches,[35] the thesis finds that there is no strong evidence of any antagonism among the three privacy regimes that pits them in a natural competition where each one claims to provide a better model than the others.[36] Instead, the thesis finds strong evidence of inter-regime complementarity, and argues that inter-regime co-operation and collaboration, which have taken various forms to this point, represent a significant feature of the pattern of interaction between the three privacy regimes. For example, the APEC Privacy Framework has relied heavily on the OECD Privacy Guidelines for its adoption of a privacy principles-based approach;[37] similarly, both the COE 108 and the OECD Privacy Guidelines were developed simultaneously based on close co-

[35] For a detailed discussion of these scholars' works, see Chapter IV, below.

[36] For the antagonistic perspective, see Chapter V, below.

[37] See OECD, "Thirty Years After: The OECD Privacy Guidelines", online: OECD <http://www.oecd.org/sti/ieconomy/49710223.pdf> ("The Guidelines have also influenced the development of the APEC Privacy Framework, expanding their reach beyond the OECD membership") at 11; see also, OECD, "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines" (1 December 2010), online: OECD <http://www.oecd.org/sti/ieconomy/theeconomicsofpersonaldataandprivacy30yearsaftertheoecdprivacyguidelines.htm>.

operation.[38] Therefore, special attention is paid to the complementary dimension of inter-regime co-operation, where some of ongoing initiatives of the OECD, EU and APEC,[39] particularly those related to transnational enforcement co-operation, information sharing and implementation collaboration, have shown evidence of moving from soft laws towards hard. The prevailing convergence on a privacy principles-based approach, initially established by the COE 108 and the OECD Privacy Guidelines, illustrates that proposition as this approach has been progressively incorporated into various national privacy and data protection legal frameworks.[40]

However, this doesn't mean that hard law is the only viable way forward for the future of international privacy and personal data governance. Hard law, as illustrated by the EU model, plays an important role but comes with its own challenges, as does the soft law. These observations, drawn on extensive theoretical analysis, animate the thesis's argument for an institutionalization of inter-regime co-operation, with a view, ultimately, to a gradual shift towards hard-law formation. The unique advantage of this gradual hardening is that it evolves through a cordial and less confrontational channel and allows all of the three privacy regimes to evolve independently and collectively, in the same normative sphere. This contention challenges the argument for the Europeanization of international privacy and personal data governance, as well as any outright demand for developing a new, strong, legally binding international framework. Thus, the thesis argues for a middle path that recognizes the importance of a theoretically-informed argument for regime complementarity, backed by the existing empirical evidence. Chapter V and VI develop these arguments further.

---

[38] See Michael Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy" (2011) 1:1 International Data Privacy Law 6 ("Above all, we drew on the regional work of the Nordic Council, the Council of Europe, and the European Communities Commission") at 10.

[39] See e.g. the ongoing collaboration between the EU and APEC though a joint APEC-EU Working Group "to foster interoperability between the APEC-CBPR and EU-BCR systems." See APEC Electronic Commerce Steering Group, online: APEC <http://www.apec.org/groups/committee-on-trade-and-investment/electronic-commerce-steering-group.aspx> [EU-APEC Interoperability].

[40] E.g. the APEC Privacy Framework adopted the privacy principles-based approach set out by the OECD Privacy Guidelines. For a critique of both the OECD Privacy Guidelines and the APEC Privacy Framework, in particular over the privacy principles, see, Graham Greenleaf, "Five Years of the APEC Privacy Framework: Failure or Promise?" (2009) 25 Computer L & Sec R 28 [Greenleaf, "Five Years of the APEC Privacy Framework"].

3) The third analytical component involves the US-EU confrontations over transborder data flows. Chapter II introduces the basic phenomenon of transborder data flows and its international governance framework, whereas Chapter III focuses specifically on the EU Data Directive 95/46/EC measures requiring a third-country adequacy assessment, measures which represent a primary reason for the ongoing US-EU confrontations. Further, Chapter V analyzes the US-EU confrontations, in particular the Safe Harbor agreement, from a theoretical perspective informed by the existing International Relations literature. Theoretically, the analysis of a transnational dispute resolved through a negotiated agreement falls primarily under the purview of IR scholarship. The thesis utilizes the hard- and soft- law theoretical framework presented by the legalization literature in IR to analyze the Safe Harbor agreement. Shaffer & Pollack argue that states' cooperative behavior is typically explained through power-and-interest-oriented accounts, specified in the language of variables; by contrast, they make a convincing case for the significance and relevance of both interest-based and normative dimensions of legalization.[41] They argue that both institutionalism and constructivism offer rich complementary insights to explain states' behavior where the issue involves hard- and soft-law aspects. The thesis draws on the important role of "sovereignty cost" as one of the important explanatory variables in determining the choice of hard- vs. soft law in the organization of inter/trans-national relations. Generally, sovereignty cost manifests itself in trade- and security-related international agreements. Hence, the thesis argues for the analytical utility of examining the ongoing EU-US confrontations, which involve both trade (e.g., the Safe Harbor agreement or the proposed EU-US Privacy Shield) and security (e.g., the recently concluded EU-US Umbrella Agreement) components.[42]

Specifically, sovereignty cost as an explanatory variable is operationalized to analyze the US-EU Safe Harbor agreement, particularly with the aim of accounting for the national interests that played a decisive role in the negotiation of the agreement. It is found that for the US the sovereignty cost was very high, as revealed throughout the Safe Harbor agreement negotiations. The U.S. therefore opted for the soft-law formulation ultimately embodied in the Safe Harbor agreement, instead of committing to a hard-law framework, as the EU was

[41] See Chapter V, below for a detailed discussion of Shaffer & Pollack's theoretical analysis.

[42] See Chapter III, below on EU-US confrontations.

demanding. One major implication of EU pressure to transpose the Data Directive 95/46/EC's hard-legalized regime was that this pushed the US to invoke antagonistic measures, including the pursuit of national interests at other international platforms, like working with APEC on the Cross-Border Privacy Rules system (CBPR) framework.[43] The thesis argues that the prolonged deadlock between the US and the EU over transborder data flows has implications for the overall evolution of international privacy and personal data governance around the world. Interpreted in terms of sovereignty cost, the thesis anticipates an indefinite prolongation of the current deadlock between the US and the EU. It found no convincing evidence that indicates any shift in the current US position, regardless of the recent conclusion of the EU-US Umbrella Agreement and EU-US Privacy Shield arrangement.

What are the implications of the above arguments for the feasibility of a new, legally binding international framework? The answer to the research question, based on the analysis of the three analytical components, is that the probability of the emergence of a new, legally binding international framework remains very low. This argument has implications for the ongoing Commissioners' Conference's strategies and initiatives. The pursuit of a hard-legalized international framework on privacy and data protection, as conceived by the Commissioners' Conference through the Madrid Resolution, is very unlikely to convert into a new, legally binding international framework in light of the thesis' main theoretical argument.

Thus, the thesis argues for launching efforts towards the institutionalization of inter-regime co-operation. It is important to stress that the thesis has not made any claims with regard to the

[43] See, online: cpbrs.org <http://www.cbprs.org>. The US has promoted the Cross-Border Privacy Rules system (CBPR) since the very beginning. The following statement by the FTC Commissioner, Edith Ramirez, shows the US intention:

> With personal information now moving around the world in the blink of an eye, we need pragmatic ways to bridge the gaps between different legal systems and privacy regimes. The APEC privacy rules have the potential to significantly benefit companies, consumers, and privacy regulators and move us closer to global interoperability of privacy regimes.

See also "FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region" (14 November 2011), online: FTC <https://www.ftc.gov/news-events/press-releases/2011/11/ftc-welcomes-new-privacy-system-movement-consumer-data-between>.

specific substance and process of such an institutionalization, as this falls beyond the analytical scope of this research project. Nonetheless, it is important that the proposed recommendation address some of the major concerns raised by the thesis. For example, any institutionalization efforts might do well to engage the data protection authorities, particularly for their expertise and experience. It would be a constructive platform to translate their knowledge into a repository of practical tools and working strategies from which to draw. Such an engagement would not only enhance the data protection authorities' credibility but would also consolidate their position as one of the main stakeholders in international privacy and personal data governance. Further, as institutionalization would build on ongoing inter-regime co-operation and collaboration efforts, every effort should be made to facilitate a comprehensive inter-regime dialogue aimed at further advancing the objective of international harmonization. Again, this approach can enhance the role of the three international privacy and data protection regimes in international privacy and personal data governance by bridging the existing gaps among them as well as by bringing them closer to the alliances of the data protection authorities and to other stakeholders.

Moreover, from the perspective of states' national interests, such institutionalization would advance those interests through a less confrontational, consensus-based platform. It will allow states to pursue their national interests at multiple delivery points, including strategic deployment of the data protection authorities and existing international regimes. More specifically, to apply that rationale to the prevailing US approach, this strategy allows the US to pursue its national interests at multiple vantage points. At the national level, the US will still be able to maintain its unique domestic regulatory framework intact, while at the international level it will be able to engage in multiple privacy-policy-making arenas. Under this approach, the US will be less likely to be confronted by questions of sovereign intervention and extraterritoriality, and will, at the same time, be able to protect economic and security-related interests. From the EU perspective, such an arrangement will provide the EU access to a strong international platform to influence international privacy and personal data governance, but this would be through consensus-based soft channels capable of minimizing transnational confrontations. This notwithstanding, the EU will still be able to pursue its interests through bilateral negotiations.

The recommended institutionalization of inter-regime co-operation offers a credible option for the future evolution of international privacy and personal data governance. Whether it would evolve into a UN convention or an intergovernmental panel or an inter-regime harmonization council, the shape and substance of such institutionalization would largely depend on the active engagement of the existing three international privacy and data protection regimes, commitment from the EU and the US, and participation of other stakeholders, including emerging alliances of the data protection authorities. This idea is further refined in Chapter VI.

2. Organization of the analysis—analytical approach

The design of the analysis in this research project relies heavily on the book *Designing Social Inquiry: Scientific Inference in Qualitative Research*[44] by Gary King, Robert O. Keohane and Sidney Verba (King, Keohane & Verba). First of all, King, Keohane & Verba describe what social scientists generally do when they conduct social-scientific inquiry as follows: "Somehow they observe a phenomenon, ask questions, infer information about the world from these observations, and make inference about cause and effect."[45] Further, King, Keohane & Verba set out four core characteristics of a scientific research project, namely: 1) the goal is inference, 2) the procedures are public, 3) the conclusions are uncertain, and 4) the content is the method.[46] The thesis' goal has been to take serious notice of these propositions and to follow them throughout the conduct of the research.

King, Keohane & Verba also identify four central elements of a research design: (1) a research question, (2) the theory, (3) the data, and (4) the use of the data.[47] A research question, according to King, Keohane & Verba, should satisfy two criteria. The first criterion stresses that a posed research question should be "important" in the real world. The criterion for being important is quite wide, like the topic should be "something that significantly affects many

[44] See Garry King, Robert Keohane & Sidney Verba, *Designing Social Inquiry, Scientific Inference in Qualitative Research* (Princeton, NJ: Princeton University Press, 1994) [King, Keohane & Verba] at 18.

[45] *Ibid* at 8.

[46] *Ibid* at 7-9.

[47] *Ibid* at 13.

people's life."[48] The second criterion underscores that a research project should make a specific contribution to an "identifiable scholarly literature". King, Keohane & Verba describe a social science theory as, "a reasoned and precise speculation about the answer to a research question, including a statement about why the proposed answer is correct."[49]

Also, a "theory must be consistent with prior evidence about the research question" and should be "concise and falsifiable."[50] The falsifiable objective can be achieved through the generation of observable implications, so that the theory can be tested in other data contexts, whereas conciseness can be ensured through precise statements and clearly stated predictions.[51] King, Keohane & Verba describe data as "systematically collected elements of information about the world"[52], stress a clear articulation of the process of data generation and use to generate inferences that are "unbiased", that is, "correct on average."[53] Furthermore, according to King, Keohane & Verba, collected data can help in theory improvement "by taking away some conditions if the prediction is based on many variables so that it can apply to a wider range of phenomena". At the same time, they warn that, "[w]e should not just add a restrictive condition and then proceed as if our theory, with that qualification, has been shown to be correct."[54]

To emphasize, the analytical approach adopted by the thesis draws heavily on King, Keohane & Verba's articulated prescriptions and proscriptions. The following commitments, therefore, are reflected throughout the analytical approach: insights are primarily based on observed facts; the research question identifies a very important issue area; the inferences drawn attempt to find an answer to the research question; these inferences are informed by theory and the

[48] *Ibid* at 15.

[49] *Ibid* at 19

[50] *Ibid.*

[51] *Ibid* at 19-20.

[52] *Ibid* at 23.

[53] *Ibid* at 27.

[54] *Ibid* at 21.

existing literature; collected data is utilized with a clear articulation of the context; and, finally, the answer to the research question is fully explained.

2.1. Methodology

King, Keohane & Verba clearly alerts a social scientist to be open and transparent so that the community of scholars, students and other interested people can expand on the knowledge developed. Furthermore, King, Keohane & Verba also assert that the "content of 'science' is primarily the methods and rules, not the subject matter, since we can use these methods to study virtually anything."[55] Thus, keeping in view the objectives identified earlier, every effort is made to articulate the rationale of the analytical approach throughout the work.

The main sources of data are strictly issue-dependent. The data is collected from both primary and secondary sources. The primary sources include treaties, conventions, case law and other legal-regulatory instruments, whereas the secondary sources include books, articles, research papers, reports, and online sources. The thesis utilizes both library and online resources. The internet sources include blogs, news media outlets, and the websites of experts and international organizations. Although the thesis takes note of the issue's historical dimensions, in light of the chosen research question, the primary focus is on recent and ongoing events. The main research objective is to produce a scholarly work that generates unbiased inferences which are correct on average, and that maximizes efficiency by using relevant information from the collected data to improve inferences.[56]

2.2. Research objectives and contribution to the literature

The main research objective underlying this research project is to understand, and explore solutions to, a very important international policy challenge related to privacy and data protection. As the problem under investigation has a global dimension, demand for the development of a global solution seems a reasonable response, particularly since the existing toolkit of governance in this area—generally composed of national and international legal and

[55] *Ibid* at 9.

[56] *Ibid* at 15.

regulatory measures—has grown increasingly weak or, in some cases, outdated and redundant. To illustrate, in response to the ongoing Snowden revelations, the EU initiated various measures and raised concerns about the reach of the US surveillance program, leading up to the ECJ's *Schrems* decision, and it was primarily for the reasons of the gaps in the existing legal frameworks.[57]

King, Keohane & Verba's exhortation underscores that in order to make a contribution to the literature, a research question has to "explicitly locate the research design within the framework of the existing social science literature."[58] Keeping that objective in mind, conscious efforts are made to situate this research project in a broader scholarly literature that informs it. On a broad level, the thesis adopts an interdisciplinary approach to the issue, situating the research as a contribution to the broad literature on the relationship between international relations (IR) and international law (IL) scholarship. On a substantive level, the research, particularly as conceived in terms of its three analytical components, draws on the literatures in political science on global governance and non-state actors, regimes and institutions, and international legalization. The section that follows reflects broadly on the relationship between IR and IL, whereas Chapters IV and V elaborate on the more specific, substantive literatures. In a review essay, Christopher C. Joyner succinctly captures the symbiotic relationship[59] between international law and international politics whereas Anne-Marie Slaughter (Slaughter) stresses the importance of the interdisciplinary synergy.[60]

---

[57] See David Wright & Reinhardt Kreiss, "European Responses to the Snowden Revelations: A Discussion Paper" (December 2013), online: irissproject.eu <http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf>. See also, *Schrems* decision, *supra* note 8.

[58] See King, Keohane & Verba*, supra* note 44 at 16.

[59] See Christopher C. Joyner, "Review: International Law is, as International Relations Theory Does?" (2006) 100:1 AJIL 248 ("The unmentionable fact is that international law and international politics are intertwined in a symbiotic relationship. Governments need political trade-offs to secure the creation, adoption, and implementation of international legal rules; national decision-makers need the means and measures of international law to conduct their foreign policies….") at 248.

[60] See Anne-Marie Slaughter Burley, "International Law and International Relations Theory: A Dual Agenda" (1993) 87 AJIL 205 [Slaughter, "Dual Agenda"] (Slaughter stresses, "[j]ust as constitutional lawyers study political theory, and political theories inquire into the nature and substance of

It is clear that the right to privacy and data protection encompasses a wide array of instruments, among them the legal-regulatory measures that are a central focus of this research. However, the inquiry is not narrowly fixated on a specific privacy law or regulation. Rather, it engages the broader privacy and personal data governance framework, with a primary focus on the three international privacy and data protection regimes; it also considers national frameworks wherever those are deemed necessary to explain the context. Furthermore, these legal-regulatory instruments are primarily created through political processes. Understanding these political processes requires insights beyond the typical legal orientation; in the international context it directly connects to the IR scholarship that has tried to explain and theorize the underpinnings of the evolution of international legal-regulatory instruments. The scope of this IR scholarship is vast, but the thesis has sought to carve out some of the specific theoretical strands relevant to capturing and explaining the phenomenon under investigation. It is the issue-context, as well as empirical observations about the role of the three analytical components, that have defined and directed the nature and scope of the theoretical literature chosen. For example, in Chapter IV, where the data protection authorities are analyzed, the literature on non-state actors and global governance (specifically that focused on transgovernmental networks) is considered most relevant, whereas in Chapter V the literature on regimes, institutions, and legalization are all considered broadly pertinent, though the legalization literature is found to be the most appropriate of all.

The study of the relationship between international law and international relations has been dominated by a complex theoretical debate[61] as to whether international politics dictates, manipulates or pervades international law, or whether law controls or structures international politics. No single answer to this debate is possible.[62] Kenneth W. Abbott (Abbott) stresses that

---

constitutions, so two disciplines the study laws of state behavior seek to learn from one another. At very least, they should aspire to a common vocabulary and framework of analysis that would allow the sharing of insights and information") at 205.

[61] *Ibid* at 206.

[62] For an extended discussion of the IR/IL tradition, see Robert J. Beck, "International Law and International Relations: The Prospects for Interdisciplinary Collaboration" (1995) 1 J Int'l Legal Stud 119; ———, "International Law and International Relations: A Scheme for Classifying Their Literatures" (2000) 94 American Society of International Law, Proceedings of the Annual Meeting 211.

the "IR theory is most helpful in performing three different, though equally significant, intellectual tasks: *description, explanation and institutional design* (emphasis in original)."[63] He underscores the important role of IR in describing legal institutions with attention to the significance of the "political factors that shape law: the interests, power, and governance structures of state and other actors; the information, ideas and understandings on which they operate; the institutions within which they interact."[64] The conceptualization and explanations presented in Chapters IV and V draw heavily on the IR literature, particularly the literatures on transgovernmental networks and legalization. Sovereignty cost as an explanatory variable is operationalized in terms of its implications for legalization; this conceptual framework is used to develop theoretical propositions out of empirical observations.

It is well established that IR scholarship is open to explaining political behavior, in particular, from the legal perspective. Again, Abbott underscores about the IL/IR relationship that "[i]t is here—constructing law-based options for the future…—that lawyers can play their greatest role and IR can make its most significant contribution."[65] Abbott further emphasizes that the legal character of international co-operation is a significant political phenomenon.[66] In a similar line of thought, Slaughter underscored that the "postulates developed by political scientists concerning patterns and regularities in states' behavior must afford a foundation and framework for efforts to regulate that behavior."[67] To read that insight in the context of this thesis: it is one of the central premises of the thesis that the analysis of past EU-US confrontations should reveal patterns and explanations sufficient to infer and anticipate the posturing of both the EU and the US. The thesis draws these insights from the IR scholarship and applies them to the context of privacy and data governance, aiming to explore the feasibility of developing a new regime.

---

[63] See Kenneth W. Abbott, "Symposium on Method in International Law: International Relations Theory, International Law, and the Regime Governing Atrocities in Internal Conflicts" (1999) 93 AJIL 361 [Abbott, "Symposium"].

[64] *Ibid* at 362.

[65] *Ibid* at 363.

[66] *Ibid* at 364.

[67] *Ibid* at 205.

From a political scientist's perspective, Slaughter further asserts that "if law—whether international, transnational or purely domestic—does push the behavior of states towards outcomes other than those predicted by power and the pursuit of national interests, then political scientists must revise their models to take account of legal variables."[68] This insight is reflected in the premise underlying the examination of the second analytical component, where the impact of existing international privacy and data protection regimes is considered. Although those existing regional regimes are international legal regulatory instruments designed primarily to harmonize national legal frameworks of member states, they are, at the same time, creations of states to address a common problem. Slaughter explains how the emergence of regime theory in 1980s, which she contends was later subsumed by "institutionalism" as an alternative to realism, has established the relevance of international law in international relations.[69] It seems clear that the interdisciplinary research alliance between international law and international relations is sufficiently well developed that its conclusions can be applied without necessarily being preceded by a survey of the literature's historical trajectory.[70]

In the end, "interdisciplinary cross-fertilization must flow both ways",[71] this means that a research project conceived at an interdisciplinary crossroads, like the present one on IR-IL, must aid both political science and legal scholarships.[72] King, Keohane & Verba suggest that a

---

[68] Slaughter, "Dual Agenda", *supra* note 60 at 206.

[69] *Ibid*.

[70] See Anne-Marie Slaughter, "International Law and International Relations Theory: a New Generation of Interdisciplinary Scholarship" (1998) 92 AJIL 367; ———, "International Law and International Relations Theory: Twenty Years Later" in Jeffrey L. Dunoff & Mark A. Pollack, eds, *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (Cambridge, UK: Cambridge University Press, 2013); ———, International Law and International Relations Theory: A Prospectus*,* in Eyal Benevisti & Moshe Hirsch, eds, *The Impact of International Law on International Co-operation* (Cambridge: Cambridge University Press, 2004); Kenneth W. Abbott, "Modern International Relations Theory: A Prospectus for International Lawyers" (1989) 14 Yale J Int'l L 335; Robert Keohane, "International Relations and International Law: Two Optics" (1997) 38:2 Harv Int'l LJ 487.

[71] See Abbott, "Symposium", *supra* note 63 at 364.

[72] See Steven R. Ratner & Anne-Marie Slaughter, eds, "Symposium on Method in International Law: A Special Issue of the AJIL" (1999) 93 AJIL 291 ("*International law and international relations* (IR/IL)

contribution to the literature can be made in one of the following ways: (1) by arguing that an important topic has been overlooked in the literature or (2) by showing that theories or evidence designed for some purpose in one literature could be applied in another literature to solve an existing but apparently unrelated problem.[73] Keeping those twin objectives in mind, the thesis aims to add theoretical knowledge in the following areas.

1. Conceptualization of privacy and personal data protection governance.
2. Descriptive account of international privacy and personal data frameworks.
3. Account of the role of the privacy enforcement authorities in international privacy and personal data governance.
4. Account of the role of international privacy and data protection regimes in international privacy and personal data governance.
5. International relations scholarship on regimes, institutions and legalization.
6. International relations scholarship on transgovernmental networks and global governance.
7. Interdisciplinary analysis of the intersection between international politics and international law.

2.3. Synopsis

Chapter I, *Introduction*, presents a detailed overview of the thesis. It summarizes the main argument of the thesis and articulates the main research question and research outcomes. The interdisciplinary nature of the thesis and its overall research design are then discussed in detail. The introduction concludes with a synopsis of the thesis.

Chapter II, *Foundation of privacy law*, aims to provide a general overview of privacy and personal data governance. This includes a detailed discussion of the general nature of the issue along with the proposed conceptualization of privacy and data protection. Further, the chapter

---

is a purposefully interdisciplinary approach that seeks to incorporate into international law the insights of international relations theory regarding the behavior of international actors") at 294.

[73] See King, Keohane & Verba, *supra* note 44 at 17.

sheds light on the general structure and substance of the national and international privacy and personal data frameworks.

Chapter III, *Privacy and data protection in global information age: Challenges, strategies and solutions,* introduces the central analytical components of the thesis. First, it reflects on the nature of the problem and then explores options for its resolution. Further, the Chapter discusses each of the three analytical components comprehensively, with a primary focus on ongoing international efforts to address the emerging challenges to privacy and personal data governance.

Chapter IV, *Data protection authorities' role in privacy and personal data governance,* examines the role of the data protection authorities in international privacy and personal data governance. By situating the data protection authorities in a broad literature on transgovernmental networks, the thesis explores the strengths and limitations of the data protection authorities in national and international privacy and personal data governance. It concludes with a brief reflection on the research question.

Chapter V*, International privacy and data protection regimes and the US-EU confrontations over transborder data flows,* conducts an analysis of these two analytical components, with a view to assessing the role and implications of the existing three international privacy and data protection regimes and ongoing US-EU confrontations over transborder data flows in the development of a new, legally binding international framework on privacy and data protection. The legalization literature is relied on extensively for conceptual and explanatory theoretical insights that are further applied and operationalized in the course of the analysis. In the end, the chapter explores the implications of its conclusions for the posited research question.

Chapter VI, *Conclusions, research outcomes, suggested alternatives, and further studies,* sums up the thesis. First comes a brief summary, where a reflection on the overall research design and objectives is reintroduced. Next follows a detailed discussion of the conclusions reached vis-à-vis the three analytical components. This leads to an examination of the answer the thesis provides to the research question it began with. Then, an argument about recommended alternatives is presented. Finally, the thesis ends with brief observations about the potential utility of applying its analytical approach to other, similar issue-areas.

Chapter II. Foundation of privacy law

The main analytical objective of this chapter is to provide a detailed insight into to the fundamentals of privacy and personal data governance. This involves two aspects. The first aspect deals with the conceptual framework. Here the primary focus will be on the notion of privacy in the personal data context, generally described as information privacy.[74] The second aspect presents a broad overview of the national and international privacy and personal data governance framework. It aims to provide the groundwork for Chapters III-VI organized analysis of the issue.

1. Conceptual framework[75]

> Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy.[76]

Privacy defies precise definition. Alan Westin stressed that "[n]o definition of privacy is possible, because privacy issues are fundamentally matters of values, interests and power."[77] Daniel J. Solove considers it a puzzling phenomenon[78] whereas Colin J. Bennett contends that,

---

[74] See generally, online: Wikipedia, Information privacy law <https://en.wikipedia.org/wiki/Information_privacy_law>.

[75] This section draws on the discussion of the concept of privacy in my LL.M. research paper.

[76] See Daniel J. Solove, "Conceptualizing Privacy" (2002) 90 Cal L Rev 1087 at 1088 [Solove, "Conceptualizing Privacy"]. See also Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale LJ 421 at 422.

[77] See Alan F. Westin, *Privacy and Freedom* (New York: Atheneum 1967) [Westin, "Privacy and Freedom"].

[78] See Solove, "Conceptualizing Privacy", *supra* note 76 (considering, "[t]he widespread discontent over conceptualizing privacy persists" at 1089).

"[p]rivacy is a notoriously vague, ambiguous and controversial term that embraces a confusing note of problems, tensions, rights and duties."[79] Generally, privacy as a human right is recognized in various international human rights instruments[80] and national frameworks.[81] Also, privacy can be classified according to specific contexts, like privacy with reference to property, person or personal information. For example, Samuel Warren and Louis Brandeis conceptualized the right to privacy as the "right to be left alone".[82]

For the thesis's analytical purposes, the notion of information privacy or privacy of personal information/data offers the most suitable conception.[83] David Flaherty provides an instrumental approach by defining 'data protection' as an aspect of privacy protection that particularly involves the "control of the collection, use and dissemination of personal information."[84] Moreover, Flaherty defines "personal information" as any information that identifies a person in whatever context and by whatever means.[85] But the most important definitions for the thesis's purposes are the ones provided by the three international privacy and data protection regimes.

---

[79] See Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, New York: Cornell University Press, 1992) at 12-13; see also, David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989) at xiii [Flaherty, "Protecting Privacy"].

[80] See e.g. the *Universal Declaration of Human Rights (UDHR)*, 1948 (Article 12) online: *UDHR* <http://www.un.org/en/universal-declaration-human-rights/>.

[81] Generally, it is recognized as a fundamental right under most constitutional instruments. For example, the Canadian *Charter of Rights and Freedoms* under Section 8 provides protection against unreasonable search and seizure. See online: Justice Laws, *Constitution Act, 1982* <http://laws-lois.justice.gc.ca/eng/const/page-15.html>.

[82] See Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193.

[83] For critical evaluation of the informational privacy aspect, see Kent Greenawalt, "Privacy and Its Legal Protection" (1974) 2:3 The Hastings Center Studies, The Future of Individualism 55-67. For excellent criticism of information privacy theory, see Paul M. Schwartz, "Charting a Privacy Research Agenda: Responses, Agreements, and Reflections" (2000) 32 Conn L Rev 929.

[84] See Flaherty, "Protecting Privacy", *supra* note 79 at xiv. See also, Robert Ellis Smith, *Privacy* (New Jersey: Archer/Doubleday 1980) at 323.

[85] See Flaherty, "Protecting Privacy", *supra* note 79 at 31.

The OECD Privacy Guidelines has stipulated in Part One, Article 1(b) that "'personal data' means any information relating to an identified or identifiable individual (data subject)";[86] this definition is applicable to both public and private sectors to the extent that they engage in processing of personal information. The COE 108, Section 1.01, Article 2 (a), defines personal data as, "any information relating to an identified or identifiable individual ('data subject')" and specifies the right to privacy "with regard to automatic processing of personal data relating to him ('data protection').[87] Article 2 (a) of the Data Directive 95/46/EC states:

> For the purposes of this Directive, 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[88]

Furthermore, the APEC Privacy Framework, Part-ii, section 9 defines personal information as "any information about an identified or identifiable individual."[89] These very similar information privacy definitions will be treated as the most representative. Given the variance in the European and other non-European countries' nomenclature, the thesis uses the combined term, like "privacy and personal data", "privacy and personal information", "data protection and privacy", "privacy", and other formulations quite flexibly. The OECD Privacy Guidelines' attached Explanatory Memorandum succinctly elaborates the terminological differences in the following terms:

> Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (lois sur la protection des données), whereas in English speaking countries they are

[86] See OECD Privacy Guidelines, *supra* note 16.

[87] See COE 108, *supra* note 18 Article (1).

[88] See EU Data Directive 95/46/EC, *supra* note 19.

[89] See APEC Privacy Framework, *supra* note 20.

usually known as "privacy protection laws.[90]

2. Privacy and personal data governance—general framework

The issue of personal data and privacy has been addressed through a wide range of national and international measures. Generally, at the national level, the right to privacy is dealt with through a wide spectrum of measures, like human rights instruments, constitutional documents, specific statutory measures, judicial interpretations, and other regulatory instruments.

Allen Westin (Westin) observes a general evolutionary pattern of privacy governance. He identifies four phases of privacy development: 1945–60, 1961–1979, 1980–1989, and 1990–2002.[91] The thesis expands on this periodization with an additional fifth phase that covers 2003-2015. Westin further highlights three core independent factors that underpin privacy development, namely: (1) new technologies and their applications by organizations, (2) social climate and public attitudes, and (3) organizational policies and laws.[92] He stressed that the period from 1961-79 was essentially embryonic, in the sense that the seeds of information privacy were sowed during that period, with society coming to recognize the rise of "information privacy as an explicit social, political, and legal issue of the high-technology age."[93] As to the third phase (1980–1989), he described it as a "period of relative calm before the storm" without "fundamental changes in information-society relationships bearing on privacy."[94]

However, the most important phase was the fourth phase (1990-2002) where privacy, according to Westin, became a "first-level social and political issue in the United States,

[90] See OECD Privacy Guidelines, *supra* note 16, Explanatory Memorandum.

[91] See Westin, "Dimensions of Privacy", *supra* note 168 at 431.

[92] *Ibid* at 434.

[93] *Ibid* at 436.

[94] *Ibid* at 438.

assumed global proportions, and was impacted by 9/11 and its aftermath."[95] He further highlights five significant developments encompassing the rise of the internet in the mid-1990s: the arrival of wireless communication devices, the technology-privacy interface, the advancement and application of data-mining software in a wide range of contexts by both private and public sectors, and the critical implications of strong encryption programs for federal law enforcement and national security agencies.[96]

Moreover, it would be reasonable to add a fifth phase (2003-2015), the so-called age of Facebook, Twitter, WikiLeaks, and Google, wherein personal information witnessed an unpredictable expansion with unprecedented privacy ramifications. The four features, *inter alia*, worth consideration in this regard are: 1) the penetration of the internet into our day-to-day lives with the rise of the "cyber-generation", such that a substantial segment of humanity now spends a considerable portion of its time in the virtual world; 2) the emergence of the internet and other information and communication technologies (ICT) as a major service delivery platform in activities like banking, shopping, travelling, and recreation; 3) massive employment of personal-information-processing tools by governments, private sectors, business entities, and the like via the ICTs, internet and computer technology — leading to heightened concerns and negative consequences such as data breaches and unauthorized or illegitimate exploitation; and 4) the omnipresence of personal data caused by the exponential increase in transnational data flows. The evolving information age is transforming our lives way beyond anything we could have imagined. The following discussion presents a general introduction to the existing system of national and international privacy and personal data governance.

2.1. National frameworks

Colin Bennett[97] identifies four main models of privacy governance: 1) a licensing model (e.g.,

[95] *Ibid.*

[96] *Ibid.*

[97] Colin J. Bennett is a Canadian scholar and a leading authority on privacy. His work encompasses a broad spectrum of privacy issues and has been extensively utilized for the thesis's analysis. For a general introduction to his research works see, online: Bennett <http://www.colinbennett.ca>.

Sweden, Denmark); 2) a data protection commissioner model (e.g., Canada, New Zealand); 3) a registration model (e.g., UK); and 4) a self-help and voluntary compliance model (e.g. the US).[98] Raab and Koops offer an interesting framing by describing the privacy and data protection from the actors' perspectives, as shown in the following table:

Table 12.1 Actors and their privacy roles and responsibilities[99]

Constitution-maker: Stipulate the right to privacy
Legislature: Make privacy-compliant laws and data protection acts
Data protection authority: Supervise and enforce compliance, encourage good practice, raise awareness in public and politics
Court: Decide cases involving privacy breaches
Government department or agency: Compliance, staff training in privacy protection
Private company: Compliance, staff training in privacy protection
Privacy activist organization: Campaign for privacy, propose regulations, raise public awareness
Academic: Explains privacy and data protection, discern long-term developments
Journalist: Highlights issues and events, explain policies and developments
Consumer: Protects own privacy, complain
Citizen: Protect own privacy, complain
Technology developer: Implement privacy-enhancing technologies (PETs), educate IT professional staff about privacy right to privacy in digital age.

From a classificatory perspective, the approach of Banisar and Davis[100] is also worthy of consideration. They categorize national regulatory frameworks in terms of three main models: the comprehensive, the sectoral and the self-regulatory.

[98] See Colin Bennett, "The Governance of Privacy: New Zealand in Global Perspective", online: Bennett <http://www.colinbennett.ca/Presentations/WellingtonMay2010.pdf> [Bennett, "Governance of Privacy"].

[99] See Charles D. Raab & Bert-Jaap Koops, "Privacy Actors, Performances and the Future of Privacy Protection" in Serge Gutwirth, eds, *Reinventing Data Protection?* (Dordrecht: Springer 2009) [Raab & Koops] 207 at 215. This article offers extensive coverage of the broad landscape of privacy and data protection governance.

[100] See David Banisar & Simon Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments" (1999) 18 J Marshall J Computer & Info L 1 [Banisar & Davis].

2.1.1. Comprehensive laws

Many countries around the world have adopted comprehensive privacy laws that generally cover both public and private sectors. Comprehensive laws, according to Banisar and Davis, are "data protection laws which comprehensively govern the collection, use and dissemination of personal information by both the public and private sectors."[101] This approach is prevalent among EU member countries. Gallman [102] provides a similar definition, describing comprehensive laws as "omnibus legislation establishing broad standards seeking to provide the best legal protection governing the collection, use, and dissemination of personal information by both the public and private sectors."[103]

According to Banisar and Davis, a key feature of a comprehensive model is a supervisory body, generally known as a Regulator, Commissioner, Ombudsman or Registrar,[104] to monitor compliance and to investigate complaints under a prescribed jurisdiction. Moreover, the supervisory body also fulfills other duties, like public awareness, representations in front of courts and other administrative bodies, annual reporting to legislature, powers of enforcement, sub-delegation, and so on. The best example of this working model is the United Kingdom *Data Protection Act, 1998*.[105]

One important subset of the comprehensive law model is described as the co-regulatory approach, adopted by countries like Canada[106] and Australia.[107] Under this model, supervisory

---

[101] *Ibid.*

[102] See Robert Gellman, "Fragmented, Incomplete, and Discontinuous: the Failure of Federal Privacy Regulatory Proposals and Institutions" (1993) VI Software LJ 199.

[103] *Ibid.*

[104] See Banisar & Davis, *supra* note 100 at 13.

[105] See online: legislation.gov.uk <http://www.legislation.gov.uk/ukpga/1998/29/contents>. See also, the UK Information Commissioner's Office, online: ICO <http://www.ico.org.uk/>.

.

[106] See *PIPEDA*, *supra* note 29. For details on the Canadian approach, see the Office of the Privacy Commissioner of Canada (OPC), online: priv.gc.ca <http://www.priv.gc.ca/index_e.asp>.

authorities' powers are limited in terms of enforcement and generally recommendatory in nature. With respect to the private sector, generally a self-regulatory approach is followed, supplemented by model codes, guidelines, principles, and practices. A supervisory authority generally monitors and investigates the application and enforcement of self-regulatory measures. If any data breach happens, the supervisory body provides recommendations, while leaving it open for the complainant to pursue recourse to civil remedies through regular court litigation. One good illustration of this model is discussed in the European Commission's recent decision on its adequacy assessment of New Zealand's national legal framework for privacy and personal data. The decision states:

> There are a number of regulatory frameworks in New Zealand for dealing with privacy issues in terms of policy, rules, or complaints jurisdictions. Some are statutory while others are self-regulating industry bodies, including media regulation, direct marketing, unsolicited electronic messages, market research, health and disability, banking and insurance and saving.[108]

It is important to note that the EU Data Directive 95/46/EC's compliance requirement does not mean that there should be a general comprehensive law, but rather states may have supplementary sectoral laws and still meet the EU Data Directive 95/46/EC requirements. Paragraph 23 of the Data Directive 95/46/EC's preamble specifically clarifies that:

> Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectoral laws such as those relating, for example, to statistical institutes.[109]

2.1.2. Sectoral laws

---

[107] See online: Federal Register of Legislations, *Privacy Ac*t 1988 <https://www.legislation.gov.au/Series/C2004A03712>. See also the Office of the Information Commissioner of Australia, online: OIC <https://www.oaic.gov.au>.

[108] See EUR-Lex, Access to European Union Law, online: EUR-Lex <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:028:0012:0014:EN:PDF>.

[109] See EU Data Directive 95/46/EC, *supra* note 19 at para 23.

Sectoral laws refer to privacy and data protection approaches that consist of targeted legislation. Under this model, countries have adopted sector-specific legislation to govern specific privacy and personal data related activities falling under those laws. The best example in this regard is the US model, which has sector-specific laws, like for video rental records, financial privacy, telephone records, heath information records, etc.

Banisar & Davis criticize this approach for lack of oversight, lags in regard to changes in circumstances, and constant updating.[110] This approach is subject to criticism for being fragmented by a set of patchwork arrangements. However, the sectoral approach has proven to be useful in addition to comprehensive laws approach, by establishing targeted legislations over specific sectors. For example, the US *Video Privacy Protection Act*[111] of 1988 prevents wrongful disclosure of video rental records, and the *Fair Credit Reporting Act* establishes rules for "consumer information contained in the files of consumer reporting agencies."[112]

2.1.3. Self-regulatory approach

Apart from these models, there exists a third approach, described as the self-regulatory model, wherein model codes, guidelines and best practices are assumed capable of constituting effective governing instruments on their own, without any government oversight at all. It is pure industry self-regulation without any external supervisory intervention. This practice has emerged as the most popular alternative in the internet context, where most of the activities are primarily based on self-regulation. The US adopted this approach with regard to a wide range

[110] See Banisar & Davis, *supra* note 100 ("A major drawback of this approach is that it requires new legislation to be introduced with each new technology so protections frequently lag behind") at 14.

[111] See online: Legal Information Institute, *Video Privacy Protection Act* <https://www.law.cornell.edu/uscode/text/18/2710 >.

[112] See online: Legal Information Institute, *Fair Credit Reporting Act* <https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-III>. For an extensive critique of the US approach, see also Paul M. Schwartz, "Preemption and Privacy" (2009) 118:5 Yale LJ 902 ("This essay argues, however, that it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law. In a sectoral approach, a privacy statute regulates only a specific context of information use."), online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1404082>.

of online activities and allowed the private sector to self-govern, as illustrated by the privacy polices adopted by internet service providers, like Google.[113]

The main criticism of this practice is the lack of oversight and substantial inadequacy of the self-governing instruments. Certainly it is the weakest form of privacy protection, but it can be a stepping-stone towards recognition and development of new privacy related arenas. Banisar has criticized this approach, adopted by the United States, Japan and Singapore.[114] With regard to the US, a study conducted by the Federal Trade Commission (FTC) in 1998 questioned the effectiveness of the self-regulation approach to protecting privacy on the internet,[115] yet the US has stuck to its position.

2.2. Regional privacy regimes

According to Westin's periodization, the recognition of the issue of privacy and personal data protection in the context of transborder data flows can be traced back to the 1980s, when advances in computer and information technology enhanced data-processing capacities. Deep-rooted sensitivity towards collection and handling of personal data in the backdrop of memories of World War II triggered national demands for regulatory controls over personal information. The Land of Hesse, Germany, was the first place to introduce privacy law in 1970, followed by Sweden (1973), the United States (1974), Germany (1977) and then other countries introducing similar legislation. One of the major policy challenges for national legislatures and policy makers has been to ensure privacy protection not only when the information stays within national borders but also when such personal information leaves or

[113] As a general practice, most of the US based websites self-govern with privacy policies mentioned on their websites. For example Google has provided it privacy policy, "Google Privacy Policy", online: Google <https://www.google.com/policies/privacy/>.

[114] See Banisar & Davis, *supra* note 100 at 23; for extensive insight into the US approach, see also Daniel J. Solove, A Brief History of Information Privacy Law, GWU Law School Public Law Research Paper No. 215, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271>.

[115] See Federal Trade Commission, "Privacy Online: A Report to Congress" (June 1998), online: FTC <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> ("To date, however, the Commission has not seen an effective self-regulatory system emerge" at 41).

has to leave its territory. Recognizing the possibility of transnational confrontations over transborder data flows as a consequence of divergent national laws, both the COE 108 and the OECD Privacy Guidelines were designed to preempt such contention through the harmonization of member countries' national frameworks. The following analysis presents a brief introduction to the three leading international privacy and data protection regimes, with a specific focus on measures to deal with transnational data flows.

2.2.1. OECD Privacy Guidelines (1981, 2013)

Though the OECD Privacy Guidelines of the 1980s were reviewed in 2013, the fundamentals stipulated by the original Privacy Guidelines of 1981 still form the basic structure. The Revised Privacy Guidelines are further discussed in Chapter III; this section presents a general overview of the Privacy Guidelines of 1981 (the OECD Privacy Guidelines). To reiterate, it was the fundamental objective of ensuring free flow of information across borders without imposing unnecessary restrictions that triggered international initiatives both at the OECD and EU in the early 1980s. "There is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers"[116], declares the preface of the OECD Privacy Guidelines. The consequent divergence among national legal frameworks was one of the fundamental considerations making it "necessary to develop Guidelines which would help to harmonize national privacy legislation." And the working strategy to achieve that harmonization objective took the form of "a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."[117] The Guidelines took the form of a recommendation by the Council of the OECD.[118]

The general framework of the OECD Privacy Guidelines consists of five parts: 1) General definitions; 2) Basic principles of national application; 3) Basic principles of international application, free flow and legitimate restrictions; 4) National implementation; and 5)

[116] See OECD Privacy Guidelines, *supra* note 16, Preface.

[117] See OECD Privacy Guidelines, *supra* note 16.

[118] *Ibid.*

International co-operation. Parts 1 and 2 are of a general nature, setting out definitions, scope and eight principles. Of special importance are Parts 3 and 5 because they provide for the international framework regarding transnational data flows and lay down provisions for enforcement and international co-operation measures.

Part 3, Basic Principles of International Application: Free Flow and Legitimate Restrictions, covers free flows of personal data among member states. It prescribes restrictions on data flows where another member country does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. It also covers "certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection."[119]

Part 4 in paragraph 19 specifically provides for a flexible range of alternatives available for a member country to comply with the Guidelines. It states:

> In implementing domestically the principles set forth in Parts Two (Principles) and Three (Free Flow and Legitimate Restrictions), Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavor to:
>
> a) adopt appropriate domestic legislation;
> b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
>
> c) provide for reasonable means for individuals to exercise their rights;
>
> d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

[119] *Ibid*, Part Three, paras 17-18.

e) ensure that there is no unfair discrimination against data subjects. [120]

Part 5, International Co-operation, stresses information-sharing on observance of the Privacy Guidelines and elaborates on mutual assistance in procedural and investigative matters. It aims to ensure "that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries."[121] Overall, the OECD Privacy Guidelines set the stage for the development of a harmonized international privacy protection approach that can be relied upon by any nation. The built-in flexibility of the Privacy Guidelines has been the major factor behind their international recognition beyond the OECD member countries.[122]

2.2.2. EU data protection regime

2.2.2.1. COE 108

Again, the objective of this section is to present a general introduction to the COE 108 and the Data Directive 95/46/EC. The COE 108 came into existence with its approval by the Committee of Ministers on September 17, 1980. Its main objective is to establish basic principles of data protection to be enforced by the member countries, to reduce restrictions on transborder data flows between the contracting parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the Convention.[123]

The most significant contribution of the COE 108 in international privacy and data protection

---

[120] *Ibid*, Part Four.

[121] *Ibid* at paras 20-21.

[122] For an extensive discussion of the role and influence of the OECD Privacy Guidelines, See 30 Years After: the Impact of the OECD Privacy Guidelines, online: OECD <http://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm> [OECD, "Impact of the OECD Privacy Guidelines"].

[123] See COE 108, *supra* note 18.

is that it was the first international instrument with legally binding obligations set out in its provisions (and the additional Protocol). It is open to accession by any non-EU country. At present, 45 Council of Europe members out of 47 have ratified the COE 108.[124]

The Preamble of the COE 108 underscores some of the important considerations, such as the recognition of the right to privacy as a fundamental freedom, freedom of information regardless of frontiers and the need "to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples…"[125] Chapter I of the COE 108 covers objectives, purpose, definition, and scope. The purpose states that:

> The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")[126].

Chapter II lists the basic principles for data protection in Articles 4-11. It lays down a broad framework for data protection, including duties of the parties, safeguards, sanctions, and remedies. Chapter III covers transborder data flows in Article 12. "Transborder flows of personal data and domestic law" sets out the conditions and restrictions for transborder data flows in the following terms:

> 1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
>
> 2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

[124] See J.-Ph. Walter, "The Role of Convention 108 in the International Cooperation", online: COE <http://www.coe.int/t/dghl/standardsetting/DataProtection/Articles/Phaedra%20workshop%20varsovie, %20J-Ph%20W.pdf>; See also the Council of Europe Events, online: COE <http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp>.

[125] See COE 108, *supra* note 18, Preamble.

[126] See COE 108, *supra* note 18.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph:

i) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

ii) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.[127]

Chapter IV covers mutual assistance (Articles 13-17) and the general approach towards co-operation and assistance. Chapter V establishes a consultative committee while Chapter VI provides for the amendment procedure and Chapter VII concludes with the final clauses.

Further, the Explanatory Report is appended to the COE 108 to underscore the importance of the free flow of information, describing it as a "principle of fundamental importance for individuals as well as nations", and advocating for determination of a formula "to make sure that data protection at the international level does not prejudice this principle." [128]

In addition to the COE 108, another important instrument is the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows." [129] The Protocol is open for signature by the state signatories to the Convention. It entered into force on 1 July 2004. The Protocol contains the rules that "essentially duplicate the rules in the Directive dealing with flow of personal data to non-member states and with the competence of national

[127] *Ibid*, Chapter III.

[128] *Ibid*.

[129] See COE 108, *supra* note 18, Additional Protocol, online: COE <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626> [COE, Additional Protocol].

data privacy authorities."[130]

The official summary outlines the main objective as follows:

> The text will increase the protection of personal data and privacy by improving the original Convention of 1981 (ETS No. 108) in two areas. Firstly, it provides for the setting up of national supervisory authorities responsible for ensuring compliance with laws or regulations adopted in pursuance of the convention, concerning personal data protection and transborder data flows. The second improvement concerns transborder data flows to third countries...[131]

2.2.2.2. EU Data Directive 95/46/EC

EU Data Directive 95/46/EC substantially builds on the platform provided by COE 108. Paragraph 11 of the Data Directive 95/46/EC states that:

> Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[132]

Data Directive 95/46/EC of the European Parliament and the Council of the EU aims "to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed."[133] It was supplemented by several other instruments providing specific data protection rules in the area of police and judicial co-operation on criminal matters (ex-third pillar), including Framework

---

[130] See Bygrave, "Privacy in Global Context", *supra* note 160 at 337.

[131] See COE, Additional Protocol, *supra* note 129.

[132] See EU Data Directive 95/46/EC, *supra* note 19.

[133] See EPIC, "EU Data Protection Directive", online: EPIC <https://epic.org/privacy/intl/eu_data_protection_directive.html>.

Decision 2008/977/JHA[3].[134] It is important to note that EU Data Directive 95/46/EC is undergoing a thorough review. In what follows, a brief reflection on the present text of Data Directive 95/46/ECs' basic provisions is provided.

EU Data Directive 95/46/EC has provided one of the most comprehensive frameworks to date for the protection of the "right to privacy with respect to the processing of personal data."[135] One of the primary objectives of EU Data Directive 95/46/EC is to ensure that the member states of the EU "shall neither restrict nor prohibit the free flow of personal data between Member States."[136] Moreover, Data Directive 95/46/EC establishes a key strategy for ensuring the free flow of information without any national legal obstacles: through the requirement of achieving an "equivalent" level of protection based on an "approximation of national laws."[137] By recognizing the existing divergence among member countries' data protection laws, the EU Data Directive 95/46/EC stresses the "need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner…"[138]

The overarching objective of Data Directive 95/46/EC is to ensure free flow of information within the EU, but it has also recognized a potential and indeed need for free flow of personal data beyond the EU member states, that is, in third countries. With respect to non-member country data flows, it has provided a general framework to help member states design national legal strategies that comply with the EU Data Directive 95/46/EC requirements. One of the major aims of the third country data flow provisions is to address concerns about the circumvention of EU member countries' national laws as well as to block the creation of data havens. Again, it is important to reiterate the thesis research focus is on Data Directive 95/46/EC, being replaced by the recently concluded GDPR, discussed in the following Chapter III.

---

[134] See EUR-Lex, online: EUR-Lex <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT>.

[135] See EU Data Directive 95/46/EC, *supra* note 19 at para 1.

[136] *Ibid,* Article 1(2)

[137] *Ibid* at para 9-10.

[138] *Ibid* at para 8.

EU Data Directive 95/46/EC has 7 Chapters consisting of 34 Articles. Chapter I, General provisions, is comprised of four Articles covering objects, definitions, scope, and national law applicability. It is important to highlight the main objectives:

> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

This objective is fairly similar to the OECD Privacy Guidelines and COE 108. The objective of balancing the right to privacy with the free flow of personal data is highlighted throughout as the central consideration of international privacy and data protection regimes. In Chapter II, Articles 5-21 lay down general rules on the lawfulness of the processing of personal data. This chapter lists fundamental principles that articulate the "conditions under which the processing of personal data is considered lawful."[139] The nine sections listed are: principles relating to data quality (section i); criteria for making data processing legitimate (section ii); special categories of processing (section iii); information to be given to the data subject (section iv); data subject's right of access to data (section v); exemptions and restrictions (section vi); data subject's right to object (section vii); confidentiality and security of processing (section viii); and notification (section ix).[140]

Chapter III, Judicial remedies, liability and sanctions, consists of Articles 22-24, whereas Chapter IV, Transfer of personal data to third countries, includes Article 25 and 26. These latter articles have proven to be the most controversial aspect of the Data Directive, as they have generated transnational confrontations as a result of their imposition of very stringent requirements on third countries. To elaborate, Article 25 imposes a requirement on a member

[139] *Ibid*, Article 5.

[140] *Ibid*, Sections i-ix.

country to ensure that before data of EU citizens are transferred to a non-member country, it must confirm that the "third country in question ensures an adequate level of protection."[141] Then, it sets out the process for assessing the adequate level of protection, as discussed in detail above. Furthermore, the Commission is equipped with the power to negotiate with a non-compliant country to remedy the situation by following the procedure referred to in Article 31 (2). Member states are bound to comply with the Commission's decisions in this regard.[142]

Article 26 lays down a framework for derogations from Article 25. It identifies certain circumstances in which transfers of personal data to a third country that does not ensure an adequate level of protection may take place, on the condition that, inter alia:

> a) the data subject has given his consent unambiguously to the proposed transfer; or
>
> b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
>
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
>
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
>
> (f) the transfer is made from a register that according to laws or regulations is intended to provide information to the public…[143]

In addition to these exclusions, paragraph 2 of Article 26 also permits personal data transfers to

[141] *Ibid*, Article 25 (1).

[142] *Ibid*, Article 25 (6).

[143] *Ibid*, Article 26.

a country with inadequate protections in situations "where the controller [of the data] adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses." [144] In any authorization of data transfers granted under paragraph 2, the member has to notify the Commission and other members. The Commission also concludes that when it has decided that certain standard contractual clauses offer sufficient safeguards, member states shall take the necessary measures to comply with the Commission's decision.[145]

Chapter V deals with the development of codes of conduct for various sectors in compliance with Data Directive 95/46/EC. Chapter VI sets out the provisions for the establishment of national supervisory authorities and of a joint working party on the protection of individuals with regard to the processing of personal data. Article 28 mandates the constitution of a national supervisory authority and outlines their functional positions. Article 29 establishes a Working Party (Working Party) with an "advisory status" and the capacity to act "independently". Further, Article 30 establishes the powers of the Working Party. Chapter VII consists of the Community implementation measures. Article 31 sets out the provisions for formulation of a Committee to assist the Commission. Article 32-34 covers the final provisions.

In conclusion, a brief reflection on the EU Data Directive 95/46/EC provisions reveals a stringent normative framework. Since the enunciation of Data Directive 95/46/EC, it has mobilized a massive legislative overhaul drive within the EU. Outside of the EU, Data Directive 95/46/EC's third country provisions have garnered international attention, leading to US-EU confrontations and to adaptations in various national legal frameworks.

2.2.3. APEC Privacy Framework

The APEC Privacy Framework (APEC Framework) emerged through a joint effort of Australia and New Zealand as a response to the emerging clout of the EU data protection regime. Prior

[144] *Ibid*, Article 26 (2).

[145] *Ibid*, Article 26 (4).

to the enunciation of the Privacy Framework, the APEC member countries randomly drew on the existing regional regimes, like the OECD Privacy Guidelines or EU Data Directive 95/46/EC. The primary reason for APEC's late response in addressing the issue of privacy and data protection was its lack of recognition of the value of privacy, which it largely considered as an impediment to economic growth and trans-border trade. Nonetheless, the Privacy Framework finally became reality in 2004. The APEC Privacy Framework is designed "to promote a consistent approach to information privacy protection, avoid the creation of unnecessary barriers to information flows, and remove impediments to trade across APEC member economies."[146]

The Foreword to the APEC Privacy Framework recognizes its overarching economic rationale in asserting that the "APEC member economies realize the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce."[147] In terms of transnational data flows, it emphasizes that, "[A] framework to enable regional data transfers will benefit consumers, businesses, and governments."[148] It further stresses the balancing aspect by "recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region."[149]

The Privacy Framework is consists of four Parts: Part I states the preamble; Part II lays down the scope; Part III lists nine information privacy principles; and finally Part IV deals with

---

[146] See APEC Privacy Framework, *supra* note 20. The Preamble at para 7 lays down:

> The Framework is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It does so by highlighting the reasonable expectations of the modern consumer that businesses will recognize their privacy interests in a way that is consistent with the Principles outlined in this Framework

[147] See APEC Privacy Framework, *supra* note 20, Foreword.

[148] See APEC Privacy Framework, *supra* note 20.

[149] *Ibid*.

implementation aspect, both domestic and international spheres.

Part I, the Preamble, lays down a broad context and articulates the underlying rationale of the development of the Privacy Framework. One of the main strategies underpinning the Privacy Framework was to draw on other international privacy and data protection regimes—mainly, the OECD Privacy Guidelines. The Preamble specifically expresses its approval for a privacy principles-based approach (paragraph 4) that is consistent with the core values of the OECD Privacy Guidelines" (paragraph 5).

Part II outlines the scope of the Privacy Framework and includes provisions on definitions and the application of the Framework. Part III lays down nine privacy principles, which include—preventing harm, notice, collection limitation, use of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability. Part IV deals with the implementation of the Privacy Framework; Section (A) deals with domestic measures whereas Section (B) addresses the cross-border data flows aspect. Further, Section (A) stresses the benefits of privacy protections and information flows across borders with an added emphasis on education and publication of domestic privacy protections, co-operation between the public and private sectors, focus on appropriate remedies in situations where privacy protections are violated, and mechanisms for reporting domestic implementation of the APEC Privacy Framework.

Domestically, the APEC Framework provides for a broad flexibility with regard to the adoption of national polices and regulatory instruments, ranging from the creation of comprehensive laws with central regulatory authorities to multi-agency enforcement authorities to business-approved self-regulatory oversight approach. The Privacy Framework is explicit about the diversity of available options, including "legislative, administrative, industry self-regulatory or a combination of these methods under which rights can be exercised under the Framework."[150] Insofar as the interests of relevant stakeholders are concerned, a balance-based approach is stressed. Remedies for the violations, equally involve a broad flexibility.[151] The

[150] See APEC Privacy Framework, *supra* note 20, Part-iii at para 31.

[151] *Ibid* at para 38.

following excerpt from paragraph 31 articulates this flexibility:

> There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative, industry self-regulatory or a combination of these methods… the Framework is meant to be implemented in a flexible manner that can accommodate various methods of implementation...[152]

In conclusion, the APEC Privacy Framework has significantly relied on the OECD Privacy Guidelines, particularly on the principles-based approach. It has adopted a wide flexibility on the implementation and enforcement measures, rather contrary to the EU Data Directive 95/46/EC's[153] stringent approach. The ultimate goal behind that flexibility is to develop compatibility of approaches in privacy protections in the APEC region that is respectful of requirements of individual economies, while recognizing the availability of different means to give effect to the APEC Framework.[154] On cross-border data transfers, the member countries are asked to co-operate with national regulatory authorities of the other member countries. The APEC Privacy Framework has adopted additional measures in recent years, discussed further in the following Chapter III.

2.3. Other international human-rights instruments on privacy

The preceding discussion illuminates the dominant approaches on privacy and personal data governance. Earlier, the conceptualization section has also emphasized the inherent conceptual complexity encompassing various dimensions of privacy.[155] Besides these privacy governance arenas, other sites where right to privacy has been given substantial recognition are briefly

---

[152] *Ibid* at para 31.

[153] For example, as seen earlier, Article 25 of the EU Data Directive 95/46/EC imposes stringent conditions on third country data transfers.

[154] See APEC Privacy Framework, *supra* note 20, Part iii at para 32.

[155] For an excellent discussion of the legal history of privacy, see Irwin R. Kramer, "The Birth of Privacy Law: A Century since Warren and Brandeis" (1990) 39 Cath U L Rev 703.

discussed as follows. The foundational international documents declaring privacy as a fundamental human right are:

1) The *Universal Declaration on Human Rights,* Article 12 declares that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[156]

2) The *International Covenant on Civil and Political Rights*, Article 17(1)[157] prescribes for:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

3) The *European Convention on Human Rights,* Article 8(1)[158], titled as, "Right to Respect for Private and Family Life", states that:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

In addition to the above three main international human rights instruments, other major international developments on privacy and data protection involve the UN adoption of the Guidelines Concerning Computerized Personal Data Files (UN Guidelines) in 1990. These UN Guidelines aimed to establish the basic "principles concerning the minimum guarantees that should be provided in national legislations."[159] Even though, some scholars have criticized the

---

[156] See *UDHR, supra* note 80.

[157] See, *International Covenant on Civil and Political Rights,* online: UN Human Rights <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [*ICCPR*].

[158] See online: *ECHR* <http://www.echr.coe.int/Documents/Convention_ENG.pdf> [*ECHR*]. See also online: Wikipedia, *European Convention on Human Rights* <https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights>.

[159] See UN General Assembly, "Guidelines for the Regulation of Computerized Personal Data Files" (14 December 1990), online: refworld.org <http://www.refworld.org/pdfid/3ddcafaac.pdf>.

UN Guidelines for "little practical effect relative to the O.E.C.D. Guidelines"[160], they matter for their importance in establishing global recognition to privacy protection efforts.

Other major development worth consideration at the UN level encompasses the right to privacy from digital age perspective. In this regard the UN initiated various measures that began with the adoption of the Resolution 68/167 by the General Assembly. The Resolution 68/167[161], also sub-titled as, "The Right to Privacy in the Digital Age"[162], calls upon all states: "To respect and protect the right to privacy, including in the context of digital communication… to take measures to put an end to violations of those rights and to create the conditions to prevent such violations…"[163] The Resolution 68/167 sets the foundation work on digital privacy with the recognition that:

> Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy…[164]

Another significant step undertaken by the UN involves the appointment of the UN special Rapporteur on the Right to Privacy[165], which marks a very significant event at the UN level

---

[160] See Lee A. Bygrave, "Privacy Protection in a Global Context–A Comparative Overview" (2004) 47 Scand Stud L 319-348 [Bygrave, "Privacy in Global Context].

[161] See the UN General Assembly, Resolution 68/167, online: General Assembly <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167> [Resolution 68/167].

[162] See the UN Human Rights Office of the High Commissioner, "The Right to Privacy in the Digital Age", online: UN Human Rights <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx> [Privacy in the Digital Age].

[163] Resolution 68/167, *supra* note 161.

[164] *Ibid*.

[165] See the UN Human Rights Office of the High Commissioner, "Special Rapporteur on the Right to Privacy", online: UN Human Rights <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx> [Rapporteur on the Right to Privacy].

with an enhanced focus on right to privacy. The UN Human Rights Council through the Resolution 28/16[166] appointed the special Rapporteur with an extensive mandate that includes, *inter alia*:

> To gather relevant information, including on international and national frameworks, national practices and experience, to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection, including in connection with the challenges arising from new technologies…[167]

In overall, the UN seems to have expanded its role in international privacy and data protection arena through some of the above-highlighted initiatives, like the appointment of the special Rapporteur on the Right to Privacy. It has also called upon to states for an enhanced focus towards resolution of privacy issues in an evolving digital age, in light of the technological advancements and increased state surveillance activities. Now, the following chapter further narrows the focus on three international arenas, in order to take stock of the *status quo* of the evolving international privacy and personal data governance.

[166] See UN Resolution 28/16 on Privacy Rapporteur, *supra* note 208.

[167] For extensive details on the Privacy Rapporteur, see online: Rapporteur on the Right to Privacy, *supra* note 165.

Chapter III. Privacy and data protection in global information age: Challenges, strategies and solutions

This chapter involves two main analytical sections. The first section presents a broad-brush assessment of the complexity and evolving nature of the issue of privacy and data protection. The following section introduces three important international privacy governance arenas from which various solutions and strategies for addressing emerging challenges have issued. Given the specific focus of the thesis on transborder data flows, special attention is paid to the international dimension of privacy and personal data governance.

Overall, this chapter aims to achieve two main objectives. First, by providing a broad overview of the nature and scope of the challenges characterizing this issue, it makes a case for exploring new solutions and strategies. The issue of privacy and data protection is placed in a broader context of the evolving global information society, with special emphasis given to the growth of data breaches and the exploitation of personal information. A discussion of some of the issues' main characteristics follows. These include a significant human rights dimension, the emergence of a common interest in privacy and data protection, and the widening range of stakeholders in privacy and data protection—particularly the emerging role of alliances of privacy enforcement authorities.

Second, by taking stock of ongoing efforts to address these new challenges at the three international privacy and data protection regimes, this chapter provides an account and assessment of the current "*status quo*" of privacy and personal data governance. This helps to establish a baseline for analyzing the nature and scope of the strategies that have emerged to cope with these challenges. Such analysis will include an assessment of the feasibility of a new, legally binding regime, as well as assessments of the role of Commissioners' Conference, the existing international privacy and data protection regimes, and efforts at transnational solutions that have emerged in the context of EU-US confrontations. These aspects are further developed in Chapters IV-VI.

1. Privacy and data protection in an era of globalization

The issue of privacy and data protection evolves within a complex and dynamic context. Allen Westin captures the essence of the issue of privacy and data protection in an era of globalization.[168] In fact, free flow of information across borders has emerged one of the necessary components of the globalization phenomenon. In a globalized world driven by internet and information communication technology (ICT)[169] the flow of personal data across borders has acquired growing prominence, yet resulted in heightened concerns, particularly for its critical role in international trade and commerce,[170] business and finance,[171] international security,[172] social interactions,[173] and movement of people.[174]

The shift of the issue of privacy and data protection away from traditional territory-bound governance structures towards a globalized phenomenon with universal manifestations poses

[168] See Alan F. Westin, "Social and Political Dimensions of Privacy" (2003) 59:2 Journal of Social Issues 431 [Westin, "Dimensions of Privacy"] ("A major development in this period [1990-2002] was the globalization of the privacy issue, driven by rising worldwide communication, trade, travel, and marketing activities") at 442.

[169] The exponential growth in internet and information communication technology (ICT) has been one of the key drivers of the globalization phenomenon.

[170] In an increasingly competitive information-based economy, personal data has emerged as one of the strategic competitive assets. The leading developed economies of the world have been aggressively seeking access to, and preservation of, personal information.

[171] E.g. multinational corporations (MNC) transfer data internationally. In the same way international banking and financial institutions cannot even conduct day-to-day business without exchanging personal information of its clients across borders. The recent multinational banking heist illustrates how data breaches have global ramifications.

[172] Since the 9/11 terrorists attacks on the US, the issue of international security has brought information sharing and co-operation among nations to a new level. As terrorist activities generally involve multinational groups, there has been a perceived need for multinational investigation and information transfer.

[173] E.g. social networks such as Facebook have emerged as worldwide social platforms where people share personal information touching on many aspects of their lives. Generally globalization is defined as: "a process of interaction and integration among the people, companies, and governments of different nations, a process driven by international trade and investment and aided by information technology." For additional observations about the phenomenon of globalization, see online: Globalization101 <http://www.globalization101.org/what-is-globalization/>.

[174] Facilitating the massive levels of human immigration and migration requires transnational exchange of the personal information of the people concerned.

unprecedented challenges for a wide spectrum of stakeholders that includes privacy policy makers, regulators, legislators, multinational corporations, banking institutions, and others with an interest in the privacy of personal data. In an expanding globalized world, national regulatory instruments and governance structures have become consistently weaker and have struggled to keep pace with a rapidly evolving world in addressing an issue which stretches beyond national borders. The need to develop new instruments that engage both national and international dimensions has thus become critical.

In conclusion, there is, on the one hand the need for a free flow of information across borders, while on the other hand a need to protect privacy and personal data. Attention has therefore focused on the so-called balancing proposition,[175] which asks how one can strike the right balance between competing interests in protecting privacy and personal data versus the free flow of data across borders.

1.1. Emergence of the global information society

Whatever form our personal-information digital footprints may take, they carry the strong prospect, whether immediate or distant, of implicating or impinging upon privacy and data protection. This is illustrated in particular by advances in internet and computer technology, which have opened unprecedented avenues for locating and identifying the precise nature of our activities based on analytics or processing of personal data. The evolving global

[175] The logic of the balancing proposition is drawn from the stated objectives of existing international regimes. For example, the preamble to the APEC Privacy Framework affirms one of its main objectives to be "... [t]o balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region." For details see, APEC Privacy Framework, online: APEC <http://publications.apec.org/publication-detail.php?pub_id=390> [APEC Privacy Framework]. Similarly, the preface to the OECD Privacy Guidelines declares, "For this reason, OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data." See OECD Guidelines. Online: OECD <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

information society challenges our existing conceptual understandings, institutional structures and regulatory polices.[176]

Today virtual avatars personify us; we have Bitcoin[177] as a virtual currency; we have cyber bullies as a new breed of criminal;[178] and we have cyber war on the horizon.[179] We leave a digital footprint whenever we access any electronic device; if the device is connected to the internet or another telecommunication system, like cellular phone service, our information is accessible and available beyond our national borders and generally beyond our control. In such a fast-paced, evolving information age it is not just the service providers but also we, as consumers, who are willing to share personal information, sometimes with explicit consent but most of the time on a voluntary basis. We share our personal social profiles on Facebook, share our photos on Flickr, or subject ourselves to surveillance cameras from shopping malls to airports. Our personal information moves without our knowledge in contexts we cannot predict; it is subject to unwanted and unnoticed exploitation, with obvious implications for our privacy. The new world of big data or metadata (data about data) is on the horizon. The following excerpt from a report by the Economist further illustrates the nature of this unfolding big data world we face:

> These changes represent the dawn of a new era of "Big Data", an era in which the sheer volume of data, and data *about* data (or metadata), can reveal profound truths about the way the world works… how businesses can better compete. New data are produced every day, generated by mobile phones, global positioning satellites and social networking sites. And each time new kinds of data are born, so too are opportunities to learn from them, combine them with existing data and create new

[176] E.g. from an information perspective, privacy is conceived as information privacy, which generally encompasses the personal control of personal information whether it relates to its collection, use or dissemination. Alan F. Westin describes information privacy 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…"; see Westin, "Privacy and Freedom", *supra* note 77 at 7.

[177] See online: Bitcoin <https://bitcoin.org/en/>.

[178] See online: Wikipedia, Cyberbullying <https://en.wikipedia.org/wiki/Cyberbullying>.

[179] See online: Wikipedia, Cyberwarfare <https://en.wikipedia.org/wiki/Cyberwarfare>.

insights.[180]

This big data poses equally big challenges for privacy and data protection. Paul Ohm calls it a "database of ruin."[181] He argues that "these databases will grow to connect every individual to at least one closely guarded secret… about a medical condition, family history, or personal preference … that, if revealed, would cause more than embarrassment or shame; it would lead to serious, concrete, devastating harm."[182] We cannot stop the evolution of the global information society, as the prospects and promise for human betterment far outweigh any other concern, including privacy and data protection; yet at the same time we have to ensure that it causes minimum disruption, rationally accommodates existing values, rights and obligations, and complies with legal requirements. Now, in terms of personal data and privacy protection a reasonable level of certainty, efficiency and reliability is necessary to ensure a sustainable path for a healthy and constructive evolution of the information society. And towards that end, we have put in place a complex set of mechanisms ranging from private sector self-regulation to comprehensive laws to address privacy and data protection challenges at national, transnational, regional, and international levels. The universal manifestations of the information society and the obvious significance of its implications for the right to privacy and personal data create a need for constant monitoring and adaptation, as well as the development of new governance instruments.[183]

The implications of the globalization of information society, the internet and other communication technologies for privacy and data protection have been one of the main themes

---

[180] See The Economist, "Big Data-Harnessing a Game Changing Asset", online: SAS <http://www.sas.com/resources/asset/SAS_BigData_final.pdf>; see also online: Wikipedia, Big Data <https://en.wikipedia.org/wiki/Big_data#cite_note-130>.

[181] See Paul Ohm, "Don't Build a Database of Ruin" (23 August 2012), online: Harvard Business Review <https://hbr.org/2012/08/dont-build-a-database-of-ruin>.

[182] *Ibid*.

[183] See Will Thomas De Vries, "Protecting Privacy in the Digital Age" (2003) 18 Berkeley Tech LJ 283 ("Digital technology - computing, databases, the Internet, mobile communications, and the like - thus calls for further evolution of privacy rights… however, the scope and magnitude of the digital revolution is such that privacy law cannot respond quickly enough to keep privacy protections relevant and robust") at 285.

of the Commissioners' Conferences. The Montreux Declaration explicitly recognizes the role of information exchange in the evolution of the information society.[184]

1.2. Security vis-à-vis privacy—post 9/11 to Snowden's revelations

The 9/11 terrorists' attack on the US was a turning point in the way states conduct their surveillance activities. Although the 9/11 events had tremendous effects on the US legal regime governing the surveillance apparatus,[185] its reverberations were felt around the western world, bringing with it significant changes for domestic legal frameworks.[186] As its post-9/11 response, the George W. Bush administration launched various national security measures, including enactment of the *PATRIOT Act*, which substantially expanded the powers of US law enforcement agencies relating to intelligence gathering and terrorism; it is said to have "gutted the U.S. Constitution's Fourth Amendment concerning unreasonable search, and the Fifth Amendment concerning the protection of a person's liberty and property by means of judicial due process."[187] One critic has assessed the current of state of the US post-9/11 legal environment in the following terms: "[i]t is no longer hyperbole to refer to the current state of

---

[184] See Montreux Declaration, "The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities", online: privacyconference2011.org <http://privacyconference2011.org/htmls/adoptedResolutions/2005_Montreux/2005_M2.pdf> [Montreux Declaration] ("Recognizing that the development of the information society is dominated by the globalization of the information exchange, the use of progressively intrusive technologies of data processing and the increase of security measures …").

[185] The creation of the Department of Homeland Security and the adoption of the National Security Agency's warrantless surveillance program are some of the examples of the US initiatives. For extra details, see Declan McCullough, "How 9/11 Attacks Reshaped U.S. Privacy Debate" (9 September 2011), online: CNET <http://www.cnet.com/news/how-911-attacks-reshaped-u-s-privacy-debate/>.

[186] For example, France passed 13 anti-terrorism measures, the United Kingdom introduced the *Anti-Terrorism, Crime and Security Act* and Canada passed the *Anti-Terrorism Act*, which became law on December 18, 2001. See Ann Cavoukian, "National Security in a Post-9/11 World: The Rise of Surveillance ... the Demise of Privacy?" then the Ontario Privacy Commissioner, online: OPC <https://www.ipc.on.ca/images/Resources/up-nat_sec.pdf>.

[187] See Richard M. Abrams, "The End of Privacy: 9/11 and the Ascendancy of the Surveillance State" Japan Policy Research Institute, Working Paper No. 122 (January 2014), online: jpri.org <http://www.jpri.org/publications/workingpapers/wp122.html>.

law and personal privacy in America as something out of George Orwell's *1984* or Franz Kafka's *The Trial*."[188]

The ongoing Snowden revelations illustrate the massive capacity and reach of the state surveillance apparatus, with serious implications for the security and privacy of personal data.[189] Snowden's revelations have prompted concerns and confrontations; for example, the EU Commission launched a comprehensive initiative designed to "restore trust in data flows between the EU and the U.S., following deep concerns about revelations of large-scale U.S. intelligence collection programmes…"[190] The communication declared that the "[m]assive spying on our citizens, companies and leaders is unacceptable."[191] In an international security context, the 9/11 terrorist attacks on the US exemplify the breadth of the global terror enterprise that has now extended to multiple countries. However, from a privacy implications perspective, national measures and international agreements launched to address and prevent such attacks in future have led to massive state-led surveillance.

In response to the ensuing public outcry, various states' governments put in place certain countervailing measures to restore public confidence. Suspicions nevertheless linger because of the advances in surveillance capacities and technological capabilities. As a result, the balancing proposition—security versus privacy—engages wider public interest, raising questions about whether we want a surveillance state with or without checks and balances.

1.3. Expansion in data breaches[192]

---

[188] *Ibid.*

[189] See Snowden, "Wikipedia", *supra* note 6.

[190] See the European Commission, Press Release Database, "European Commission calls on the U.S. to Restore Trust in EU-U.S. Data Flows" (27 November 2013), online: European Commission <http://europa.eu/rapid/press-release_IP-13-1166_en.htm> [EU, "Rebuilding Trust"].

[191] *Ibid.*

[192] See e.g. the website, Information is Beautiful, which keeps track of millions of data breaches. See online: informationisbeautiful.org, World's Biggest Data Breaches <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

Aside from the two major factors highlighted above, an unprecedented increase in cases of data breaches and exploitation has emerged as one of the most formidable challenges to privacy and data protection. In global information age our personal data exist not in secure and encrypted silos but in a form accessible from anywhere in the world, provided the data processing system is connected to the Internet. Therefore, the challenge is how to protect privacy and personal data not only within national territory but also in a transnational context. The expansion of data breaches and exploitation from national to transnational/international spheres not only exposes the limits of national regulatory instruments but also requires measures capable of addressing them beyond national territorial limits. Such measures require international co-operation and harmonization of national measures, but can also lead to transnational confrontations.

Aside from state surveillance, another significant development that has resulted in massive data collection and processing is the emergence of personal information as a strategic economic asset. Today there is an open market for selling and buying personal data. Everything from our health data to our driving records to our credit card information have become hotly pursued assets.[193] Besides criminal and unwanted exploitation, new phenomena like cyber activism are emerging challenges. Take the recent example of the Ashley Madison[194] data breach where the personal data of its customers was released to the public by hackers, allegedly in order to stop the website from promoting undesirable relationships; interestingly, state authorities were unable to trace the hackers behind the releases. The international banking and finance sectors offer another good illustration of the depth of data breaches and exploitation. On February 16, 2015, USA Today reported a US $1 billion banking heist, organized through a multi-national cyber crime enterprise, which involved 30 major international banks and hackers from Russia,

[193] See Francis S. Chlapowski, "The Constitutional Protection of Informational Privacy" (1991) 71 BUL Rev 133 (noted that the "advent of the Information Age has precipitated the commodification of virtually all types of personal information") at 133.

[194] See, BBC, "Ashley Madison Infidelity Site's Customer Data 'Leaked'" (19 August 2015), online: BBC <http://www.bbc.com/news/business-33984017>. See e.g. online: Ashley Madison <https://www.ashleymadison.com/?lang=en_US&c=2&utm_source=google&utm_medium=cpc&utm_term=ashley%20madison&utm_content=e&utm_campaign=Ashley+Madison+-+CA++Brand&network=g&gclid=CLqF69HeksgCFQ6paQodVnAHbQ>.

China and European countries.[195] In another example, the Australian Federal Police have reported incidents involving international group of criminals attempting to steal money.[196]

1.4. Data privacy as a human right

Despite wide variation in the conceptualization of privacy and data protection among countries around the world,[197] what seems to be shared is a common sense that the right to privacy is primarily a human right. It encompasses individual liberties and other interests in personal information practices.[198] On right to privacy, there exists sufficient international consensus recognizing it as one of the fundamental human rights. This consensus is embodied in all three of the major international human rights instruments: the *Universal Declaration on Human Rights* (*UDHR*), the *International Covenant on Civil and Political Rights* (*ICCPR*) and the *European Convention on Human Rights (ECHR)* have all established the right to privacy.[199] Generally, the right to privacy is also recognized in constitutional documents around the world,

[195] See Mike Snider and Kaja Whitehouse, **"**Banking Hack Heist Yields up to $1 Billion" (16 February 2015), online: USA Today <http://www.usatoday.com/story/tech/2015/02/15/hackers-steal-billion-in-banking-breach/23464913/>.

[196] See e.g. the Herald Sun, "Australian Federal Police Foil Russian Crime Gang's $570m Cyber Theft Bid as Nation Loses $4.6 Billion-a-year to Computer Crime" (23 July 2014), online: Herald Sun <http://www.heraldsun.com.au/news/law-order/true-crime-scene/australian-federal-police-foil-russian-crime-gangs-570m-cyber-theft-bid-as-nation-loses-46-billionayear-to-computer-crime/news-story/6ede13d25f63a4c8c922cbe44037553d>.

[197] For extra details, see Chapter II, Conceptualization section, above.

[198] See London Declaration, "Communicating Data Protection and Making it more Effective", online:privacyconference2011.org<http://privacyconference2011.org/htmls/adoptedResolutions/2006_London/2006_L1.pdf> [London Declaration, "Communicating Data Protection"] ("As our societies are increasingly dependent on the use of information technologies, and personal data are collected or generated at a growing scale, it has become more essential than ever, that individual liberties and other legitimate interests of citizens are adequately respected in relevant information practices").

[199] For an extended discussion of international privacy and data protection instruments, see Chapter II's section on other international human rights instruments for privacy and data protection.

like Section 8 of the Canadian constitution.[200] Moreover, in 2013 Graham Greenleaf reported around 100 countries with data privacy laws.[201]

Privacy and personal data protection has also been established through other international governance instruments, as illustrated by the three leading regimes—the OECD Privacy Guidelines, the COE 108 and the EU Data Directive 95/46/EC and the APEC Privacy Framework. The OECD Privacy Guidelines underscore the "important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders."[202] This brief historical reference illuminates the significance of the right to privacy in its various international incarnations, which is a critical factor to be considered when a case is made for its international protection, whether it be through a binding international framework or otherwise.

1.5. Common interest in shared goals and objectives

The right to privacy and data protection is not only manifest in diverse contexts but also serves multiple interests and engages multiple stakeholders. Three leading international regimes—the OECD Privacy Guidelines, the COE 108 and the Data Directive 95/46/EC and the APEC Privacy Framework—explicitly recognize the joint importance of the free flow of information vis-à-vis the security of privacy and data protection. And towards that end, all three privacy and data protection regimes have sought to achieve harmonization across member states' national frameworks. Despite that common interest, international privacy and data protection regimes diverge in many respects. The EU has adopted a more stringent approach to enforcement measures, whereas the OECD Privacy Guidelines and the APEC Privacy Framework have adopted a more flexible approach. Cross-national harmonization arguably has

---

[200] See *Constitution Acts, 1867-1982*, online: Justice Laws Website <http://laws-lois.justice.gc.ca/eng/const/>.

[201] See Graham Greenleaf, "Global Data Privacy Laws 2013: 99 Countries and Counting" (2013) 123 Privacy Laws & Business International Report 10; also available online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305882>.

[202] See OECD, "OECD Work on Privacy", online: OECD <http://www.oecd.org/sti/ieconomy/privacy.htm>.

benefits in terms of cost, regulatory compliance and legal certainty. It is also important to check efforts to circumvent the legally protected right to privacy and data protection.[203]

One of the fundamental objectives behind the emergence of the three international privacy and data protection regimes has been to address the conflict of laws among member countries. This objective was illustrated throughout the deliberation process leading to the conclusion of both the OECD Privacy Guidelines and the COE 108 in early 1980s, when international negotiations over new regime construction took place.[204] Yet efforts to avoid conflicts of laws have partially failed to harmonize national responses, as reflected in ongoing trans-national confrontations. Such confrontations are due primarily to the substantial political-economic implications[205] of privacy and data protection measures, and to inter-regime divergence over implementation and enforcement. The very existence of the three separate regional regimes further projects that dynamic deeper into domestic regimes. Despite such inter-regime divergence, ongoing transnational confrontations and emerging challenges, it is critical to notice that all of the three international privacy and data protection regimes share common objectives and goals, even though they might differ in other respects on the specific approaches to adopt.

1.6. Emergence of non-state stakeholders

The globalization of the information society has diminished the state's traditional sovereign control over international issues. Today, big corporations to small retailers all participate in transnational business activities, with very high stakes for personal information. The ultimate consequence of this phenomenon is the emergence of privacy professionals, scholars, activists, NGOs, corporate lobby groups, the privacy enforcement authorities' alliances, and so on. This,

[203] See e.g. European harmonization of law, online: Wikipedia, Harmonization of Law <https://en.wikipedia.org/wiki/Harmonisation_of_law>.

[204] See OECD Privacy Guidelines, *supra* note 16 ("On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers…").

[205] See e.g. ongoing EU-US confrontations over transborder data flows, which illustrate this aspect very well.

for example, is the focus of scholarly work by Colin Bennett on privacy advocates, work which has examined the expanding role of non-state stakeholders in international privacy governance.[206] Under this paradigm shift, state governments and other entities engaged in personal-data-related activities have found themselves under closer public scrutiny, with various stakeholders voicing their concerns. Whoever deals with personal data has to deal with these stakeholders too. This thesis has focused on one such leading stakeholder, the alliances of privacy enforcement authorities, largely because the Commissioners' Conference has spearheaded the demand for a new global framework development.

This initiative of the US Centre for Digital Democracy (CDD), which seeks US FTC action against 35 corporations, demonstrates the influential role of non-state actors in a national context.[207] Similarly, in the international context, a recent March 2015 resolution (A/HRC/28/L27)[208] by the UN Human Rights Council to establish a special rapporteur on right to privacy, backed by 92 NGOs[209], exemplifies this newfound capacity of non-state stakeholders.

Thus, the widening ambit of stakeholders in privacy and data protection creates an atmosphere for a broad public dialogue that challenges existing, traditional privacy policy-making. In this

---

[206] Colin Bennett's work on privacy advocates includes a book and a dedicated website, privacyadvocates.ca. See Bennett, "Privacy Advocates", *supra* note 1; see also, online: privacyadvocates.ca <http://www.privacyadvocates.ca>.

[207] See Christopher Stevens & Stephen Holland, "How (and Why) Safe Harbor needs to be Reformed" (26 August 2014), online: IAAP <https://iapp.org/news/a/on-why-safe-harbor-needs-to-be-reformed>. This is a good example where non-state actors working together with other international non-state actors to influence national frameworks.

[208] See UN Human Rights Council, "Resolution 28/16", online: UN Human Rights <http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/L.27> [UN Resolution 28/16 on Privacy Rapporteur].

[209] EPIC, for example, participated in the NGOs representation for the establishment of the special UN Rapporteur on the Right to Privacy, see EPIC, "Joint NGOs Oral Statement to the Human Rights Council 28th Ordinary Session Call to Establish a UN Special Rapporteur on the Right to Privacy" (13 March 2015), Online: Human Rights Watch <http://www.hrw.org/sites/default/files/related_material/Joint%20NGO%20statement%20calling%20for%20a%20Special%20Rapporteur%20on%20the%20Right%20to%20Privacy.pdf>.

information age where cyber activism on a given issue can emerge rapidly and can expand on many fronts at once, it is hard to altogether ignore demands for enhanced privacy and data protection. The Global Commission on the Internet Governance (GCIG) issued a statement calling on 'the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the internet technical community, with the goal of restoring trust and enhancing confidence in the Internet."[210] Responding to this CGIC statement, Angel Gurría, the OECD Secretary-General and a member of the GCIG, asserted that "[r]estoring trust in the absence of a broad social agreement on norms for digital privacy and security is crucial. As a member of the GCIG, I welcome this call… to agree on the terms of a social compact for digital privacy and security."[211]

Although, the above discussion sketches a broad-brush picture of the nature and scope of the emerging challenges to privacy and data protection, the London Declaration[212] offers additional support for some of the observations made. The following description briefly highlights the main affirmations articulated in the London Declaration, affirmations that succinctly convey the thesis's message in a different light. The Declaration recognizes three sets of challenges: the first relates to the technology-driven globalized world; the second touches on the security dimension with special emphasis on the rise of anti-terror laws; and the third challenges some assumptions about the role of the data protection authorities. The first two aspects are briefly discussed as follows.

The London Declaration identifies six core features of technological change, along with their implications for legal frameworks. These are: acceleration; globalisation; ambivalence;

---

[210] See the Global Commission on the Internet Governance (GCIG), "Toward a Social Compact for Digital Privacy and Security" (15 April 2015), online: GCIG <https://www.ourinternet.org/publication/toward-a-social-compact-for-digital-privacy-and-security/>.

[211] See OECD News Room, "OECD's Gurría Welcomes call for 'Social Compact for Digital Privacy and Security' as Critical First Step for Trust and Economic Prosperity" (15 April 2015), online: OECD <http://www.oecd.org/newsroom/oecds-gurria-welcomes-call-for-social-compact-for-digital-privacy-and-security-as-critical-first-step-for-trust-and-economic-prosperity.htm>.

[212] See London Declaration, "Communicating Data Protection", *supra* note 198.

unpredictability; invisibility; and irreversibility. In terms of legal implications, the main challenges for privacy and data protection stem from law lagging behind the accelerating pace of technological change; the unpredictable ways in which technologies get used; the invisibility of data processing; the inability of law designed on a geographical basis to control international data flows; citizens' ambivalence towards technology's privacy implications, and the irreversibility of technological changes. The Declaration asserts that the "[t]echnological progress is irreversible: we shall never live any more in a world without computers, Internet, mobile phones… As these technologies converge and become ever-more interwoven, their combination could present real risks for our societies."[213]

The second challenge concerns the security context in a post-9/11 and post-Snowden era. The London Declaration stresses the need for balance among competing privacy and security interests; the danger of getting caught in a spiral system where the scope of databases (who is registered, who has access) constantly expands without accompanying legal authorization or supervision; the illusion of the exemplary nature of foreign precedents for surveillance systems; the mirage of the database as a miracle cure; and the myth of the infallible file, where the inclusion of the individuals registered in a database is automatically assumed to be justified. The Declaration warns that "[i[t is therefore essential, from an ethical point of view, to keep affirming that technology is fallible and to forbid automatic decision making, especially in domains such as security and justice."[214]

To conclude: on the one hand we have the emergence of a global information society with an increasing role for personal information along with heightened concerns for privacy and data protection, whereas on the other hand we have a growing demand for action in the wake of the unprecedented increase in the incidence of data breaches and unwanted exploitation of personal data. Added to the complexity is the increased public focus on privacy issues, whether

[213] *Ibid*.

[214] *Ibid*.

due to the ongoing spat between the FBI and Apple[215], the further entrenchment of cyberspace into the social fabric, or the unprecedented penetration of the surveillance system. The major implication of this complex, evolving phenomenon is that it has challenged the existing legal-regulatory frameworks with raising serious concerns over their effectiveness and their capacity to secure privacy and data protection. What policies and regulatory frameworks should be developed for an effective resolution of these emerging privacy and data protection challenges? The following section examines three relevant arenas, each representing a potentially viable option, from which various strategies and solutions are emerging.

2. Solutions and strategies—three international arenas of action

In addition to the preceding observations about the evolving nature of the issue, other important factors requiring consideration are the conceptualization of privacy and data protection, the emergence of a wide range of governance measures, ranging from self-regulation to co-regulation to comprehensive laws, and the prevailing divergence among national legal frameworks and international regimes. Such a complex and evolving issue context makes it nearly impossible to specify the issue in clear terms and that, by implication, puts existing governance approaches and strategies in perennial catch-up mode.

Given that complexity, the dominant trend in international privacy governance toward an expanding patchwork of solutions is very problematic for three main reasons. First, an emerging patchwork of solutions at the level of the three international regimes further weakens the capacity of existing international arrangements to develop coherent and harmonized solutions. This, by extension, undermines the common objective to strike an appropriate balance between the free flow of information across borders and adequate privacy and personal data protection.[216] Second, the growing divergence among the international privacy and data

[215] See Dave Lee, "Apple v FBI: US Debates a World without Privacy" (2 March 2016), online: BBC <http://www.bbc.com/news/technology-35704103>; see also Kalev Leetaru, "Why The Apple Versus FBI Debate Matters In A Globalized World" (2 March 2016), online: Forbes <http://www.forbes.com/sites/kalevleetaru/2016/03/02/why-the-apple-versus-fbi-debate-matters-in-a-globalized-world/#5c93fdda2639>.

[216] This objective has been well recognized in all three international privacy regimes. For example, the OECD Privacy Guidelines explicitly recognizes "that although national laws and policies may differ,

protection regimes further extends to the national regulatory frameworks; hence the consequential rise in trans-national confrontations.[217] And third, it creates opportunities for unwanted exploitation of personal information, whether it is by state governments, criminals or commercial entities, without facing the substantive force of law.[218] Thus, the trajectory of influence from international to regional to national levels offers the disturbing prospect of the adoption of a lowest threshold or of a "race to the bottom", with adverse ramifications for privacy and personal data protection. Whether we look from a top-down or bottom-up perspective, the existing state of international privacy and data governance, with its pattern of deepening divergence, has created the conditions for a further weakening of privacy and data protection. One recent example can be found in the EU's frustration and strong protest against the US's massive, ongoing NSA surveillance program.[219] The following quote illustrates this pattern:

> European citizens' trust has been shaken by the Snowden case, and serious concerns still remain following the allegations of widespread access by U.S. intelligence agencies to personal data. Today, we put forward a clear agenda for how the U.S.

Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information." See OECD Privacy Guidelines, online: OECD <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[217] The problem of divergent national laws for privacy and data protection and their implications for transborder data flows has been one of the central considerations behind international initiatives in the early 1980s leading to the conclusion of the COE 108 and the OECD Privacy Guidelines. The OECD Privacy Guidelines recognizes in their Preface that "there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers..." and stressed that the "OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data." See also OECD Privacy Guidelines, *supra* note 16.

[218] This is because the divergence among existing international privacy and data protection regimes and domestic legal frameworks creates an opportunity for many countries around the world to settle on a lowest threshold for the adoption of a weak privacy and data protection legislative framework; hence, it creates an opportunity for data havens, transnational confrontations and other forms of unwarranted exploitation.

[219] See e.g. the recent decision of the ECJ in *Schrems* case, which further illustrates the EU's frustration. For extra details, see, *Schrems* decision, *supra* note 8.

> can work with the EU to rebuild trust, and reassure EU citizens that their data will be protected. Everyone from the internet users to authorities on both sides of the Atlantic stand to gain from co-operation, based on strong legal safeguards and trust that these safeguards will be respected," said Cecilia Malmström, European Commissioner for Home Affairs.[220]

How to address the ever-expanding divergence among national and international privacy and data protection regimes? How to mitigate the rise in transnational confrontations over transborder data flows? The need to search for solutions seems obvious. Could that solution be a new, overarching international regime? Or could it be an overhaul of the existing international privacy and data protection regimes? Or could the *status quo* provide the best way forward? In the past, the international community has shown a will to act together on the issue of privacy and personal data protection, as the adoption of the Council of Europe Convention 108[221] and the OECD Privacy Guidelines[222] (discussed in detail in the following section with other international initiatives), later updated by the EU Data Directive 95/46/EC and joined by the APEC Privacy Framework in 2004, all seem to suggest.[223] Also, all three of the leading international privacy and data protection regimes have launched various measures to address the emerging challenges.

Moreover, various privacy scholars, experts, advocates, and other stakeholders have recommended a wide range of options.[224] For example, De Hert, Paul, Papakonstantinou, and

---

[220] See EU, "Rebuilding Trust", *supra* note 190.

[221] See COE 108, *supra* note 18.

[222] See OECD Privacy Guidelines, *supra* note 16.

[223] See APEC Privacy Framework, *supra* note 20.

[224] For an extended discussion of a wide range of suggestions, see Bygrave, "Privacy in Global Context", *supra* note 160; Robert Gellman, "Can Privacy be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules" (1996) 41:1 Vill L Rev 129 [Gellman, "International Privacy Rules"]; Joel R. Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace" (2000) 52.5 Stan L Rev 1315; Colin Bennett, "An International Standard for Privacy Protection: Objections to the Objections", The Internet Law and Policy Forum, online: ilpf.org <http://www.ilpf.org/events/jurisdiction2/presentations/bennett_pr/>.

Vagelis suggested three options, namely: 1) maintaining the *status quo* and relying on technology to address public concerns, 2) the new EU general data protection regulation emerging as a global standard, and 3) developing an international data privacy organization, preferably under UN auspices.[225] On the other hand, others have raised doubts about the prospects for the emergence of a new, binding international legal instrument.[226] Christopher Kuner, after a thorough analysis of the available options, concludes that "[t]he time does not yet seem ripe for a binding international legal instrument on data protection…"[227] Given this difference in opinions, the thesis will explore all of these possibilities.

In the following discussion, the thesis examines three international arenas where various initiatives are emerging. First, it deals with the Commissioners' Conference initiatives, which demanded the development of a new, legally binding international framework. It is followed by an assessment of the initiatives at the level of the international privacy and data protection regimes and concludes with emerging transnational measures between the EU and the US, specifically in the context of transborder data flows.

2.1. New regime development—the Commissioners' Conference initiatives

Before analyzing the efforts to develop a new regime, it is necessary to reflect on the rationale behind these efforts. A quick appraisal of the gravity and expansive nature of the ongoing challenges to privacy and personal data might appear to provide clear support for the proposition to pursue the creation of a new regime. However, it does not mean that this is the only viable option to consider. A search for solutions should canvass a more complex set of considerations than the common sense assumption articulated in the rationale for pursuing development of a new international framework. Nonetheless, that proposition does possess

[225] See De Hert Paul & Papakonstantinou Vagelis, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?" (2013) 9:2 I/S: A Journal of Law and Policy for the Information Society 270 [Hert & Vagelis].

[226] See e.g. Kuner, "International Legal Framework", *supra* note 2 (recognized that "a binding international legal instrument covering data protection would be premature…") at 310.

[227] *Ibid* at 316.

special value, in that it sets a clear challenge to the international policy making community, all the while inviting stakeholders to participate in a broader public dialogue.

The Commissioners' Conference has emerged as one of the strongest voices pushing for the development of a new, legally binding international framework.[228] Typically, such a venture would fall under the traditional sovereign domain of states, but the process of globalization along with the ICT revolution have created unprecedented opportunities for non-state actors to forge international alliances designed to influence outcomes in international privacy governance.[229] The Commissioners' Conference has formed a strategic alliance with various non-state actors to mobilize national and international policy makers to address the increasing challenges to privacy and data protection. Moreover, the Commissioners' Conference has emerged as a leading voice advocating that national governments join the initiative to develop a new global standard. It has also appealed to the UN to organize an international convention and advocated for the organization of an intergovernmental conference to develop a legally binding international instrument.

In the following discussion, the Commissioners' Conference's initiatives are analyzed. The main objective of this analysis is to briefly describe the nature of the forum and to survey its major initiatives, as embodied in the various resolutions it has adopted. The descriptions and observations articulated in this section will be drawn on in the analyses of Chapters IV-VI, where a closer examination of the role of the data protection authorities in privacy and personal data governance will be conducted.

It is important to understand the basic concept of a privacy regulator, privacy commissioner or data protection authority. A wide range of descriptive terms that varies from country to country is used to designate a privacy protection authority. In Canada, the term is privacy

[228] See the International Conference of Data Protection and Privacy Commissioners (ICDPPC), official website, online: ICDPPC <https://icdppc.org> [ICDPPC Website] ("The Conference seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of about 110 privacy and data protection authorities from across the globe").

[229] See e.g. the annual gathering of the Commissioners' Conference engages various stakeholders through open public discussions over wide range of issues relating to privacy and personal data governance.

commissioner; in Germany, it is the data protection commissioner; in Norway, the data inspectorate; elsewhere in Scandinavia, the ombudsman; and in the United Kingdom (UK), the information commissioner.[230] By contrast, the international privacy and data protection regimes tend to use functionally defined terms, like the EU's term "data protection authorities" and the APEC Privacy Framework's use of the term "privacy enforcement authorities". A common feature that characterizes almost all of the data protection authorities is that they are primarily administrative authorities created by a governing statute with a prescribed jurisdiction over specific issues related to privacy and personal data. As a result, the thesis utilizes these terms liberally and according to context: e.g. when the discussion focuses on the EU, it may use the term "data protection authorities" (DPAs), whereas regarding APEC; it may use the term "privacy enforcement authorities" (PEAs).

The other important consideration requiring attention is to explain why the Commissioners' Conference is central both to the thesis' research and to international privacy and personal data governance. This is primarily for two reasons. First, the Commissioners' Conference is the leading international alliance of DPAs, where privacy experts and policy makers gather annually to deliberate on wide range of issues that are important to privacy and personal data governance. Second, the Commissioners' Conference, as a leading international group of national regulatory authorities, has substantial access to, and a credible prospect of influencing, national policies. These national data protection authorities are the primary administrative bodies to address and resolve a wide range of privacy and personal data protection issues. They possess a breadth of experience and expertise that has given them a certain public credibility, allowing them to inform and engage public perception and to draw legislatures' attention to serious issues. Chapter IV discusses these matters in greater depth.

The first International Data Protection and Privacy Commissioners' Conference was held in Bonn, Federal Republic of Germany, in 1979. It mainly involved the Western European data protection and privacy commissioners. Since then, the Conference has emerged as one of the

[230] See e.g. the UK *Data Protection Act* of 1988 was modified to be in compliance with EU Data Directive 95/46/EC, while changing the title of the Data Protection Commissioner to "Information Commissioner". For extra information refer to the Wikipedia page, online: Information Commissioner's Office <http://en.wikipedia.org/wiki/Information_Commissioner's_Office>.

major international platforms to exchange information, share experience and develop strategies to address the evolving challenges surrounding the issue of privacy and data protection. The Commissioners' Conference's annual gathering is organized by a national data protection authority, selected among the members. It deliberates and delivers results through the resolutions it adopts. The Commissioners' Conference sets its own procedures and protocols involving administrative matters. Under the current format, the hosting data protection authority decides on the main theme of the Commissioners' Conference. The Commissioners' Conference generally consists of an open session accessible to all privacy professionals, a closed session only accessible to data protection and privacy authorities, and several side meetings organised by non-governmental organisations. Multiple stakeholders, including multinational corporations (MNCs) and civil society organizations, can participate in the Commissioners' Conference proceedings.[231]

2.1.1. Major initiatives of the Commissioners' Conference—Resolutions adopted (Madrid, 2005 to Amsterdam, 2015)

As highlighted above, the main delivery instruments of the Commissioners' Conference are the resolutions adopted. These resolutions generally cover a wide range of objectives, issues and strategies aimed to strike appropriate balance among competing interests.[232] Also, most of adopted resolutions engage multiple stakeholders, including the alliances of privacy enforcement authorities, non-state actors, international organizations, and national governments.

The following section surveys some of the important resolutions, with three principal aims: (1) to describe their relationship with existing international regimes; (2) to describe their

[231] E.g. EPIC, a leading US-based NGO, generally runs a parallel non-state actors conference alongside the annual Commissioners' Conference.

[232] For example, see the Warsaw Conference, "Resolution on Anchoring Data Protection and the Protection of Privacy in International Law", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/International-law-resolution.pdf> [Resolution on International Law] (the Resolution asserts: The 35th International Conference observes: that there is a pressing need for a binding international agreement on data protection that safeguards human rights by protecting privacy, personal data and the integrity of networks and enhances the transparency of data processing while striking the right balance in respect of security economic interests and freedom of expression).

relationship with national frameworks and other alliances of the data protection authorities; and (3) to analyze the strategies and initiatives adopted by the Conference, with a view to providing an answer to the research question. Analytically, this section is designed to help organize the analysis in Chapter IV, which assesses the role of the data protection authorities in privacy and personal data governance.

The following excerpt from the Strasbourg Conference (2008) succinctly captures the essence of the Commissioners' Conference's initiatives towards a legally binding instrument:

> The recognition of these [privacy] rights requires the adoption of a universal legally binding instrument establishing, drawing on and complementing the common data protection and privacy principles laid down in several existing instruments and strengthening the international co-operation between data protection authorities.[233]

This quotation articulates three central features that are critical for this analysis, namely: 1) the nature of the proposed new international instrument (universal; legally binding), 2) the sources of this instrument (data protection and privacy principles laid down in several existing instruments) and 3) the Commissioners' Conference's objective (strengthening international co-operation between the data protection authorities).

2.1.1.1. Emphasis on co-operation, coordination, collaboration, and promotion

The four objectives—co-operation, coordination, collaboration, and promotion—constitute the strategic toolset employed by the Commissioners' Conference throughout the adopted resolutions. The following discussion is organized by introducing some selected excerpts from those resolutions. The emphasis on international co-operation has been the hallmark of the Commissioners' Conference's emergence on the world stage. The groundwork was laid down

[233] See Strasbourg Conference, "Resolution on the Urgent need for Protecting Privacy in a Borderless World", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resoltuion-on-the-urgent-need-for-protecting-privacy-in-a-borderless-world.pdf> [Strasbourg Conference, "Resolution on Privacy in a Borderless World"].

in the Montreux Declaration (2005),[234] which was further developed in the annual Conferences that followed: London (2006),[235] Montreal (2007),[236] Strasbourg (2008),[237] Madrid (2009),[238] Jerusalem (2010),[239] Mexico City (2011),[240] Punta del Este

[234] See 27th International Conference on Privacy and Personal Data Protection Commissioners, Montreux, Switzerland (2005), online: Privacy Conference <http://www.privacyconference2005.org/> [Montreux Conference].

[235] See 28th International Conference on Privacy and Personal Data Protection Commissioners, London, UK (2006), online: Privacy Conference <http://www.privacyconference2006.co.uk/> [London Conference].

[236] See 29th International Conference on Privacy and Personal Data Protection Commissioners, Montreal, Canada (2007), online: Privacy Conference <http://www.privacyconference2007.gc.ca/> [Montreal Conference].

[237] See 30th International Conference on Privacy and Personal Data Protection Commissioners, Strasbourg, France (2008), online: Privacy Conference <http://www.justice.gov.il/PrivacyGenerations/adopted.htm> [Strasbourg Conference].

[238] See 31st International Conference on Privacy and Personal Data Protection Commissioners, Madrid, Spain (2009), online: Privacy Conference <www.privacyconference2009.org/home/index-iden-idweb.html> [Madrid Conference].

[239] See 32nd International Conference on Privacy and Personal Data Protection Commissioners, Jerusalem, Israel (2010), online: Privacy Conference <http://www.justice.gov.il/PrivacyGenerations> [Jerusalem Conference].

[240] See 33rd International Conference on Privacy and Personal Data Protection Commissioners, Mexico City, Mexico (2011), online: Privacy Conference <http://privacyconference2011.org/index.php?lang=Eng> [Mexico Conference].

(2012),[241] Warsaw (2013),[242] Mauritius (2014)[243] and the recently concluded Amsterdam (2015)[244] conference.

The Montreux Declaration (2005) (Montreux Declaration)[245] conceived the idea of developing a new, legally binding international framework or universal convention. It stressed enhanced international co-operation in its strategies for developing the new regime. The following excerpt from the resolution adopted highlights the main objective:

> They […Data and Privacy Commissioners] agree to collaborate in particular with the governments and international and supra-national organizations for the development of a universal convention for the protection of individuals with regard to the processing of personal data.[246]

The Montreux Declaration explicitly identified the intent of the Commissioners' Conference with a specific focus on developing a universal convention as the delivery instrument for a legally binding framework. It further appeals "to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights," as well as to "every Government in the world to promote the

---

[241] See 34th International Conference on Privacy and Personal Data Protection Commissioners, Punta del Este, Uruguay (2012), online: Privacy Conference <http://privacyconference2012.org/english/> [Punta del Este Conference].

[242] See 35th International Conference on Privacy and Personal Data Protection Commissioners, Warsaw, Poland (2013), online: Privacy Conference <https://privacyconference2013.org/> [Warsaw Conference].

[243] See 36th International Conference on Privacy and Personal Data Protection Commissioners, Mauritius (2014), online: Privacy Conference <http://www.privacyconference2014.org> [Mauritius Conference].

[244] See 37th International Conference on Privacy and Personal Data Protection Commissioners, Amsterdam (2015), online: Privacy Conference <http://www.apc2015.net/content/amsterdam-privacy-week> [Amsterdam Conference].

[245] See Montreux Declaration, *supra* note 184.

[246] *Ibid*.

adoption of legal instruments of data protection and privacy according to the basic principles of data protection."[247]

The London Initiative (2006) (London Initiative) and its declaration, **"**Communicating Data Protection and Making It More Effective,"[248] spelled out a long-deliberated strategy with a specific emphasis on the data protection authorities.[249] Section-IIB, paragraph 25, emphasizes the development of a universal convention, stresses the role of co-operation and co-ordination, and advises the DPAs that they "should endeavour to promote this initiative in their respective spheres of influence, in particular within the regional organisations or linguistic zones to which they belong."[250]

Further, the Montreal Conference (2007) (Montreal Conference) also emphasized international co-operation in the following terms:

> Recalling the Montreux Declaration that called on the United Nations to develop a legally binding instrument to protect privacy; affirmed the commitment of data protection commissioners to promote co-operation amongst themselves and with others involved in data protection; and appealed to governments to promote the adoption of legal instruments of data protection and privacy.[251]

Another significant resolution adopted at the Montreal Conference concerned "the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes."[252] The main feature of the adopted resolution was that it initiated international standard-setting, while emphasizing the role of the DPAs.

---

[247] *Ibid*.

[248] See London Declaration, "Communicating Data Protection", *supra* note 198.

[249] *Ibid*.

[250] *Ibid*.

[251] See Montreal Conference, "Resolution on International Co-operation", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-International-Co-operation.pdf>.

[252] See Montreal Conference, "Resolution on the Urgent Need for Global Standards for Safeguarding Passenger Data to be used by Governments for Law Enforcement and Border Security Purposes",

The Madrid Resolution[253] likewise stresses the importance of co-operation and coordination among the national data protection authorities. The above excerpts underscore the importance of co-operation, coordination, collaboration, and promotion with regard to the development of a new universal convention and binding legal instruments. These organizing principles permeate almost all aspects of the Commissioners' Conference initiatives. Some resolutions have clearly followed them while others have recited them through general references. The following section explores the evolutionary trajectory of the proposed binding legal instrument.

2.1.1.2. Efforts towards a new, legally binding instrument

The Montreux Declaration was the first official endorsement of the idea of developing a universal, legally binding instrument through a UN convention.[254] Since then that reference has been invoked in almost all of the subsequent Commissioners' Conferences that addressed the question of a new international framework. The Strasbourg Conference[255] adopted a very important resolution, with an emphasis "on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection."[256] (Strasbourg Resolution on Privacy in a Borderless World) Recalling the previously concluded Conferences, primarily the Montreux (2005) and Montreal (2007) Conferences, the Conference created a mandate to establish a working group composed of the interested data protection authorities to draft and submit to its closed session a

---

online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Urgent-need-for-global-standards-for-safeguarding-passenger-data-to-be-used-by-governments-for-law-enforcement-and-border-security-purposes.pdf>.

[253] See Madrid Conference resolution, "Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Data", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf> [Madrid Resolution].

[254] See Montreux Declaration, *supra* note 184 (the Conference made appeal "to the United Nations to prepare a legal binding instrument which clearly sets out in detail the right to data protection and privacy as enforceable human right…").

[255] See Strasbourg Conference, "Resolution on Privacy in a Borderless World", *supra* note 233.

[256] *Ibid.*

"[j]oint proposal for setting international standards on privacy and personal data protection."[257] It further stipulated that the working group should develop the international standards on privacy and personal data protection based on the following criteria:

> To draw on the principles and rights related to the protection of personal data in the different geographic environments of the world, with particular reference to legal and other texts that have attracted a wide degree of consensus in regional and international forums.
>
> To elaborate a set of principles and rights which, while reflecting and complementing existing texts, aim to achieve the maximum degree of international acceptance ensuring a high level of protection…
>
> To define, taking into account the diverse legal systems, the basic criteria that guarantee their effective application...
>
> To formulate the essential guarantees for better and flexible international transfers of data.[258]

Moreover, the resolution also stressed the importance of engaging various stakeholders, in particular, the International Organization for Standardization (ISO) and of the International Law Commission (ILC), with "the purpose of obtaining the broadest institutional and social consensus." [259] Therefore, the Strasbourg Conference made a strategic move towards developing a new international standard by setting up a working group with a mandate to develop such standards under the guidance of the above criteria.

The Madrid Conference (2009) (Madrid Conference) adopted the resolution "Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Data" (Madrid Resolution)."[260] The Madrid Resolution incorporated the basic

---

[257] *Ibid.*

[258] *Ibid.*

[259] *Ibid*.

[260] See Madrid Resolution, *supra* note 253.

"principles that are present in different international instruments, guidelines or recommendations of international scope and that have received a broad consensus in their respective geographical, economic or legal areas."[261] The drafting of these international standards stands central to the Commissioners' Conference's efforts towards developing a new, legally binding privacy and data protection instrument. The following discussion briefly introduces the standard developed.

The international standard is composed of seven parts and 25 sections. Part I, General Provisions, consists of sections 1-5: Purpose; Definitions; Scope of application; Additional measures; and Restrictions. Part II, Basic Principles, consists of sections 6-11, titled: Principle of lawfulness and fairness; Purpose specification principles; Proportionality principles; Data quality principle; Openness principle; and Accountability principle. Part III, Legitimacy of Processing, consists of sections 12-15, titled: General principle of legitimacy; Sensitive data; Provision of processing services; and International transfers. Part IV, Rights of Data Subject, consists of sections 16-19, titled: Right to access; Right to rectify and delete; Right to object; and Exercise of these rights. Part V, Security, consists of sections 20-21, titled: Security measures and Duty of confidentiality. Finally, Part VI, Compliance and Monitoring, consists of sections 22-25, titled: Proactive measures; Monitoring; Co-operation and coordination; and Liability.[262]

The overarching objective that the Commissioners' Conference aimed to achieve through the adoption of the Madrid Resolution was to "[demonstrate] the feasibility of such standards, as a new step towards the development of a binding international instrument in due course."[263] The other significant objective to be achieved through the Madrid Resolution was to lay down a "set of principles, rights, obligations and procedures that any legal system of data protection and privacy should strive to meet."[264] Further, the national data protection authorities were

[261] *Ibid*.

[262] *Ibid*.

[263] *Ibid*. This aspect is further developed in the main argument part of the thesis in Chapter VI, below.

[264] *Ibid.*

encouraged to disseminate and promote the Madrid Resolution as a means of encouraging development of a UN convention.[265]

The Jerusalem Conference in 2010 (Jerusalem Conference)[266] undertook a very important measure with the adoption of the "Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data."[267] Again, by recalling almost all major previous Commissioners' Conferences, and emphasizing the earlier creation of the international standard, the Jerusalem Conference renewed the demand for a universal instrument, stressing its importance and explicitly calling on "[g]overnments to organise an intergovernmental conference, in 2011, or in 2012 at the latest, in order to reach an agreement on a binding international instrument guaranteeing the respect of data protection and privacy and facilitating international co-operation in the enforcement of those legal rules."[268]

The Mexico Conference (2011) (Mexico Conference)[269] adopted various resolutions and reports, but the most important with regard to international standard development was the report titled, "Promotion of the International Standards: State of Play"[270] (State of Play). It recognized the fact that the "organization of an intergovernmental conference… has not been possible in 2011 and won't be in 2012, [though] several actions of promotion of the joint

---

[265] *Ibid*.

[266] See Jerusalem Conference, "Resolution Calling for the Organisation of an Intergovernmental Conference with a View to Developing a Binding International Instrument on Privacy and the Protection of Personal Data", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-International-Conference.pdf> [Resolution on Intergovernmental Conference].

[267] *Ibid.* The resolution assert: "An intergovernmental conference designed to reach an agreement on a binding international instrument would be another major step that would allow the fundamental breakthrough of the Madrid Resolution to become a legal and practical reality."

[268] *Ibid.*

[269] See Mexico Conference, *supra* note 240.

[270] *Ibid*. See special report, "Promotion of the International Standards: State of Play", online: Privacy Conference <http://privacyconference2011.org/index.php?lang=Eng> [State of Play].

proposal for international standards have been accomplished in 2011."[271] While no concrete measures towards such an intergovernmental conference were taken, the State of Play report reiterated that the "[c]onference will continue to promote the Joint Proposal for International Standards in all relevant international fora (e.g. OECD, Council of Europe, APEC) and its efforts to organize an intergovernmental conference for developing a binding international instrument."[272]

The State of Play report updated international standard development by stressing international co-operation on enhancing privacy enforcement and co-ordination at the international level, in the light of ongoing parallel international activities, particularly at the OECD and the APEC levels. The main resolution adopted in this regard was the "Resolution on Privacy Enforcement and Co-ordination at the International Level" [273] (Privacy Enforcement Co-ordination Resolution). The overarching objective set out in the resolution was **"**to encourage efforts to enable more effective coordination of cross-border investigation and enforcement in appropriate cases."[274] The resolution further stressed that the privacy enforcement authorities should cooperate, share enforcement experience, participate in cross-border enforcement co-operation "and, if necessary, discuss with their governments proposals to amend existing legislation to facilitate greater co-operation."[275] Furthermore, the appended explanatory note emphasizes that "[t]his resolution takes a new step by seeking to develop concrete proposals and mechanisms to facilitate enforcement coordination."[276] The resolution focuses on four areas: building upon existing co-operation measures; reviewing laws to remove barriers to co-operation; setting up a temporary working group to develop new processes for coordination;

[271] *Ibid*.

[272] *Ibid*.

[273] Mexico Conference, *supra* note 240. See also, "Resolution on Privacy Enforcement Co-ordination at the International Level", online: privacyconference2011.org <http://privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_001_%20Intl_Priv_Enforc_ENG.pdf> [Resolution on Privacy Enforcement Co-ordination].

[274] *Ibid*.

[275] *Ibid*.

[276] *Ibid*.

and occasional meetings on enforcement coordination between privacy enforcement authorities.

A noticeable shift in the Commissioners' Conference strategy can be observed in the Mexico Conference's resolutions. These resolutions seem to have shifted the focus to co-operation and co-ordination rather than pursuit of a new, legally binding international framework, as sought in previous conferences. The push for an intergovernmental conference seems to have faded or to have been set aside, and instead efforts were made to pursue solutions that are more in keeping with the thesis's central argument, presented in Chapter VI: the greater desirability of exploring inter-regime co-operation through institutionalization, rather than setting one's sights on developing a strong, legally binding international framework. The Privacy Enforcement Co-ordination Resolution further undertook:

> To establish a temporary conference working group to develop a framework and processes to share information about potential or existing investigations or enforcement actions and to facilitate possible coordination. The working group is encouraged to work in cooperation with other networks of privacy enforcement authorities active in cross-border enforcement cooperation and is directed to report back to the 34th Conference on what concrete actions have taken place over the year as well as what elements need further work and discussion.[277]

At the Punta del Este, Uruguay Conference (2012)[278] (Punta del Este Conference) the main resolution adopted was the "[r]esolution on the future of privacy"[279] (Resolution on the Future of Privacy). This resolution explicitly recognizes the European Union's ongoing discussions about "proposals for a revised legal framework for data protection", along with ongoing work and initiatives by the Council of Europe, the OECD and APEC (particularly the APEC Cross-Border Privacy Rules), US national initiatives, and the role of multilateral co-operation and

[277] *Ibid*.

[278] See Punta del Este Conference, *supra* note 134, "Resolution on the Future of Privacy", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-the-Future-of-Privacy.pdf>.

[279] *Ibid*.

enforcement networks in fostering enforcement co-operation among international privacy enforcement authorities. It concluded with emphasizing that its members should:

> 1. Intensify co-operation with each other in order to respond to cross-border data protection and privacy risks in a coordinated manner, by joining multilateral co-operation and enforcement networks.
>
> 2. Share information and expertise as much as possible to ensure that the authorities' scarce resources can be used to the maximum possible.
>
> 3. Use this window of opportunity to achieve greater interoperability between the various legal systems and privacy regimes. [280]

Again, the Punta del Este Conference explicitly recognizes the increasing significance of ongoing international developments, in particular at the international privacy and data protection regimes level. The implications of these developments seem to be that the demand for a new, legally binding international instrument has been pushed back even further.

The Warsaw Conference of 2013 [281] (Warsaw Conference) marks a major shift in the Commissioners' Conference strategy. The resolution adopted is titled, "Strategic Direction."[282] The Strategic Direction resolution sets out in Part B three main strategic priorities for the years 2014 and 2015: 1) carving a niche, 2) putting the Conference on a sustainable footing, and 3) building capacity towards a successful global network.[283] Another major resolution was the "resolution on anchoring data protection and the protection of privacy in international law."[284] The resolution added a new layer to the demand for new standard development by asking the UN to incorporate the standards on the protection of data and privacy adopted by the Madrid

---

[280] *Ibid.*

[281] See Warsaw Conference, *supra* note 242.

[282] *Ibid*. See, "Resolution on Conference's Strategic Direction", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Strategic-direction-resolution.pdf> [Warsaw Resolution on Conference's Strategic Direction].

[283] *Ibid*.

[284] See Resolution on International Law, *supra* note 232.

Declaration into an additional protocol to Article 17 of the *International Covenant on Civil and Political Rights* (*ICCPR*). By recognizing the "pressing need for a binding international agreement on data protection", the Commissioners' Conference resolves:

> To call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law.[285]

Another important resolution adopted at the Warsaw Conference was related to international enforcement coordination.[286] The resolution emphasized that the Commissioners' Conference should "encourage efforts to bring about more effective coordination of cross-border investigation and enforcement in appropriate cases."[287] This resolution again underscored ongoing developments in other arenas, in particular cross-border co-operation in the enforcement of laws protecting privacy at the OECD, the EU and the APEC levels.

The Mauritius Conference of 2014[288] (Mauritius Conference) adopted two important resolutions, namely, Resolution on Enforcement Co-operation[289] and Global Cross Border Enforcement Co-operation Arrangement.[290] The resolution on enforcement co-operation

---

[285] *Ibid*.

[286] See Warsaw Conference, *supra* note 242, "Resolution on International Enforcement Coordination", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Enforcement-coordination-resolution.pdf> [Resolution on Enforcement Coordination].

[287] *Ibid.*

[288] See Mauritius Conference, *supra* note 243.

[289] *Ibid*. See, "Resolution on Enforcement Co-operation", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/ResolutionInternational-cooperation.pdf> [Resolution on Enforcement Cooperation].

[290] See Mauritius Conference, *supra* note 243, resolution on "Global Cross Border Enforcement Cooperation Arrangement", online: privacyconference2014.org <http://www.privacyconference2014.org/media/16667/Enforcement-Cooperation-Agreement-adopted.pdf> [Resolution on Global Cross Border Enforcement].

recognized that an "increased transborder data flows should be accompanied by increased cross-border information sharing and enforcement co-operation between privacy enforcement authorities." The other main emphasis of this resolution was to advance the Global Cross Border Enforcement Co-operation Arrangement as a possible basis for facilitating co-operation between members on enforcement. Thus, the resolution on Global Cross Border Enforcement Co-operation Arrangement becomes the latest document with a significant prospect for influencing international privacy and personal data governance, as it lays the groundwork for further co-operation and coordination in cross-border enforcement measures. Interestingly, the focus of this resolution is primarily on an enhanced role for privacy enforcement authorities rather then an appeal to national governments in general:

> The purpose of this Arrangement is to foster data protection compliance by organisations processing personal data across borders. It encourages and facilitates all PEAs' co-operation with each other by sharing information, particularly confidential enforcement-related information about potential or on-going investigations, and where appropriate, the Arrangement also coordinates PEAs' enforcement activities to ensure that their scarce resources can be used as efficiently and effectively as possible.

Further it again prescribes the four central principles of co-operation, reciprocity, confidentiality, data protection, and coordination. It sets a time line and a process for its approval by at least two privacy enforcement authorities to become effective before the coming 37th conference of privacy commissioners. Thus, this resolution arguably marks a new beginning in international privacy and personal data governance, and its real effectiveness is yet to emerge.

The latest, Amsterdam Conference of 2015 (Amsterdam Conference) adopted four resolutions, namely: Resolution on Conference's Strategic Direction;[291] Resolution on Co-operation with

[291] See Amsterdam Conference, "Resolution on Conference's Strategic Direction (2016-18)", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Conferences-Strategic-Direction-2016-18.pdf> [Amsterdam Resolution on Conference's Strategic Direction].

UN Special Rapporteur on the Right to Privacy;[292] Resolution on Privacy and International Humanitarian Action;[293] and Resolution on Transparency Reporting.[294] Now, from the thesis' analytical perspective,[295] the Resolution on Strategic Direction further extends the Warsaw Conference's objectives with four strategic priorities for 2016-2018: 1) Strengthening Our Connections, Working With Partners; 2) Advancing Global Privacy in a Digital Age; 3) Completing Conference Capacity building; and 4) Assessing Our Effectiveness.

Another resolution, on co-operation with the UN Special Rapporteur on the right to privacy, stresses the need for a global solution, while emphasizing the Warsaw Conference's resolution on the adoption of an additional protocol to Article 17 of the *International Covenant on Civil and Political Rights*. It seeks an engagement of the UN Privacy Rapporteur with "data protection and privacy authorities from around the world in his work programme… [and] calls upon [him]…. to promote the start of negotiations on such a protocol within his first mandate."[296] Again, the Amsterdam Conference's focus centers on the importance of international co-operation, connections and working with other partners.

Clearly, the above-excerpts from various adopted resolutions illuminate the ongoing efforts of the Commissioners' Conference, which are not limited to mere advocacy, public awareness and information exchange. The Commissioners' Conference is moving in a direction to become the major stakeholder in international privacy and personal data governance. This intent is clearly evident in adopted multi-dimensional strategies, which encompass both international and

[292] See Amsterdam Conference, "Resolution on Co-operation with UN Special Rapporteur on the Right to Privacy", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf> [Conference Resolution on UN Privacy Rapporteur].

[293] See Amsterdam Conference, "Resolution on Privacy and International Humanitarian Action", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf>.

[294] See Amsterdam Conference, "Resolution on Transparency Reporting", online: ICDPPC <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Transparency-Reporting.pdf>.

[295] These points are further developed in Chapter IV's analysis, which explores the question of the institutionalization efforts of the Commissioners' Conference.

[296] See Conference Resolution on UN Privacy Rapporteur, *supra* note 292.

national privacy and data protection policy spheres. The following Chapter IV further expands on the increasing role of the Commissioners' Conference in privacy and personal data governance.

2.1.1.3. Strategic shift—UN convention to UN special Privacy Rapporteur and the Conference's interactivity and institutionalization

The Madrid Resolution indicates a forward-looking intent on the part of the Commissioners' Conference. More broadly by emphasizing "the Joint Proposal demonstrates the feasibility of such standards, as a new step towards the development of a binding international instrument in due course.[297] Also, the preceding discussion has highlighted the long-standing impulse to develop a new, legally binding international framework and has assessed in this regard the Commissioners' Conference's various resolutions. The discussion in Chapters IV to VI will draw on and extend these observations. In concluding the analysis at this point, however, two broad points can be made. The first emphasizes the evolutionary trajectory of the project of developing a new international regime, whereas the second concerns strategies oriented to institutionalization and to enhancing collaboration with other stakeholders.

A noticeable shift can be observed in the Commissioners' Conference strategy with regard to its ambitious project, beginning with the Strasbourg Conference, to develop a legally binding international standard, initially through a proposal for a UN convention. The Madrid Declaration was a notable success, with its adoption of a draft international standard; the follow-up at the Jerusalem Conference sought a UN intergovernmental conference. However, the shift in question emerges during the Mexico Conference that reoriented the Warsaw Conference's objectives, with a resolution that demanded the adoption of an additional protocol to Article 17 to the *ICCPR* in order "to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law."[298] Further, the Mauritius Conference put a renewed focus on international co-operation among the privacy enforcement authorities, with the adoption of a specific agreement on Global Cross Border

[297] See Madrid Resolution, *supra* note 253.

[298] See Resolution on International Law, *supra* note 232.

Enforcement Co-operation Arrangement. Finally, the latest Amsterdam Conference sought engagement with the UN Special Rapporteur on the right to privacy in order to advance the demand for adoption of the additional protocol to Article 17 of the *ICCPR*.

In terms of strategic positioning and institutionalization efforts, the Amsterdam Conference's resolution, Strategic Direction, sets out a detailed blueprint of the vision and provides for a working plan on strategic priorities for the years 2016-18. The International Conference of Data Protection and Privacy Commissioners now has a dedicated website, with a secretariat provided by the New Zealand's Office of the Privacy Commissioner. It has ratcheted up its earlier focus on enhanced co-operation with international organizations in order to "develop supportive connections between networks involved in cross-border data protection and privacy enforcement" and to "explore ways in which the Conference and regional forums of DPAs can better connect and enrich each other."[299]

Though Chapter IV presents a theoretical argument about the significant role of the privacy enforcement authorities in international privacy and personal data governance, it is important to keep these points in mind when trying to understand the evolutionary trajectory of this international alliance with high stakes in privacy and personal data governance. The following observations provide an overall gloss on the Commissioners' Conference's efforts and strategies. The first underscores the Commissioners' Conference's own institutional evolution as an international organization. The second draws attention to the venues of power that Commissioners' Conference can access in order to exert influence on privacy and personal data governance. A good illustration is the ambitious project to develop a UN convention, followed by an appeal for an intergovernmental conference, then an approach to the ILC to develop a legally binding instrument, and finally a submission to the UN to add the Madrid Resolution into an additional protocol to Article 17 of the *ICCPR*. This ambitious enterprise seems to have shifted, as indicated by its inability to execute some of its more challenging features. Moreover, rising internal skepticism might be inferred from the recent statements of the Commissioners' Conference suggesting the need to acquire power to influence national outcomes — especially in the appeals to member DPAs to try to bring about changes in their own respective national laws and policies. Underlying such appeals is an assumption that the

[299] See Amsterdam Resolution on Conference's Strategic Direction, *supra* note 291.

DPAs possess sufficient independent credibility and authority to be able to induce such national-level changes, which is questionable, given that most of these data protection authorities are statutorily created administrative bodies with delegated authority subject to judicial oversight and executive supervision. Finally, the third observation relates to the Commissioners' Conference as an international alliance of the data protection authorities that is increasingly directing its attention to expanding its interactions with other, similar privacy enforcement authorities' alliances, the existing privacy and data protection regimes and other venues of privacy policy-making. On this front the Commissioners' Conference seems to have taken cautious yet strategic moves, as revealed in the Amsterdam Conference's resolution on Strategic Direction. This is a work in progress. The following section takes stock of the other important international venue, the three international privacy regimes, with a focus on the nature and scope of their ongoing efforts to address emerging challenges to privacy governance.

2.2. Adaptation and modification of the existing international regimes

As highlighted earlier, the second option available to address emerging challenges to privacy and personal data governance is to adapt and modify the existing international regimes. This option has been a constant work in progress in the case of all three international regimes. The question whether a regime-modification approach would deliver an optimal solution is debatable because of prevailing inter-regime divergence. Despite this divergence over enforcement measures, all three of the privacy and data protection regimes converge significantly on general goals, objectives and a principles-based approach. Moreover, reflection on their ongoing measures, as assessed in the following section, points to substantial efforts towards inter-regime co-operation.

The following analysis surveys the measures adopted by each of the three international privacy and data protection regimes, with a primary focus on illuminating the thesis' research objectives and explicating the rationale underlying the regimes' adoption of those measures — particularly their emphasis on international co-operation, harmonization, co-ordination, collaboration, and inter-regime operability. The conclusions of this analysis will provide the background information and empirical context for Chapter V's analysis.

The following section introduces the measures adopted by the three international regimes. As a brief background, the Council of Europe and the OECD launched international privacy and personal data protection governance strategies in the early 1970s. Each set of efforts culminated in a distinct international privacy and data protection regime, namely, the COE 108 and the OECD Privacy Guidelines. Later, in 2000, the EU developed the Data Directive 95/46/EC, which was followed by the APEC Privacy Framework adopted in 2004. The OECD also introduced the Revised Privacy Guidelines in 2013; whereas the EU is in the final stage of introducing a new framework.

2.2.1. OECD initiatives on privacy and personal data governance

The OECD Privacy Guidelines constitute an essentially flexible framework, particularly when it comes to compliance and enforcement provisions. Nonetheless, the OECD Privacy Guidelines have had significant influence on privacy and personal data governance around the world since their inception in the early 1980s. In 2010, in response to the emerging challenges to international privacy and personal data governance, the OECD launched a comprehensive strategy to overhaul and update the existing framework. On the occasion of the 30th anniversary of its Privacy Guidelines,[300] the OECD organized four main events: 1) Roundtable on the Impact of the Privacy Guidelines (Paris, 2010);[301] 2) Conference on the Evolving Role of the Individual in Privacy Protection (Jerusalem, 2010);[302] 3) Roundtable on the Economic Dimensions of Personal Data and Privacy (Paris, 2010);[303] and 4) the OECD Conference on

[300] See OECD, "30th Anniversary of the OECD Privacy Guidelines", online: OECD <http://www.oecd.org/internet/ieconomy/the30thanniversaryoftheoecdprivacyguidelines.htm>.

[301] See OECD, "Impact of the OECD Privacy Guidelines", *supra* note 122.

[302] See OECD, "The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines", online: OECD <http://www.oecd.org/internet/ieconomy/theevolvingroleoftheindividualinprivacyprotection30yearsaftertheoecdprivacyguidelines.htm>.

[303] See OECD, "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines", online: OECD <http://www.oecd.org/internet/ieconomy/theeconomicsofpersonaldataandprivacy30yearsaftertheoecdprivacyguidelines.htm>.

Global Interoperability (Mexico City, 2011).[304] These events culminated in the adoption of the Revised Privacy Guidelines in 2013. The OECD's Working Party on Information Security and Privacy (WPISP) led the Guidelines revision process, which was based on the terms of reference[305] released at the OECD conference on global interoperability. The goal of the following discussion is to present a review of these ongoing OECD efforts.

2.2.1.1. Revised Privacy Guidelines, 2013

The Revised Privacy Guidelines involve two main instruments: the Recommendation of the OECD Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (July 2013) and a new Explanatory Memorandum providing context and rationale for the July 2013 revisions.[306]

The Revised Privacy Guidelines consists of two central themes. The first is focused on the practical implementation of privacy protection through an approach grounded in risk management, while the second stresses, "efforts to address the global dimension of privacy through improved interoperability." [307] Moreover, the Revised Privacy Guidelines also introduce three new approaches: the national privacy strategies, privacy management programs and data security breach notification. On the national privacy strategy side, aside from national laws, the role of "multifaceted national strategy co-ordinated at the highest levels of government" [308] is stressed, whereas the privacy management programs dimension encompasses "the core operational mechanism through which organisations implement privacy

[304] See OECD, "Current Developments in Privacy Frameworks: Towards Global Interoperability", online: OECD <http://www.oecd.org/internet/ieconomy/currentdevelopmentsinprivacyframeworkstowardsglobalinteroperability.htm>.

[305] See OECD, "Terms of Reference", online: OECD <http://www.oecd.org/internet/ieconomy/48975226.pdf>.

[306] See Revised Privacy Guidelines, *supra* note 17.

[307] *Ibid.*

[308] *Ibid*.

protection."[309] Also, the Revised Privacy Guidelines emphasize the objective of modernizing the OECD approach on transborder data flows. It continues to stress the importance of the original OECD Privacy Guidelines of 1981 by leaving the enshrined principles as is.

In terms of structure, the Revised Privacy Guidelines are comprised of six parts and an annexed detailed explanatory memorandum. Part One involves general provisions; Part Two lists the basic principles of national application; Part Three covers implementation accountability; and Parts Four to Six cover international and national implementation, international co-operation and interoperability. The following paragraph (17) from Part Four outlines the basic principles of international application:

> 17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.[310]

Paragraph 17 stipulates two conditions under which a country should refrain from blocking free flow of data transfer to a third country, and it is quite wide and flexible in its assessment of those two conditions. Further, Paragraph 18 provides for a proportionality principle as follows:

> 18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.[311]

Part Five lays down a framework for ensuring that a state's national measures are in compliance with the conditions of the Revised Privacy Guidelines regarding data transfer. Paragraph (19) (a-i) sets out the conditions member countries must observe:

---

[309] *Ibid.*

[310] *Ibid.*

[311] *Ibid.*

a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;

b) adopt laws protecting privacy;

c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;

d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

e) provide for reasonable means for individuals to exercise their rights;

f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;

g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures, which help to protect privacy;

h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and

i) ensure that there is no unfair discrimination against data subjects.[312]

The Revised Privacy Guidelines seem to present a generalized version of an effective national privacy and data protection framework; however, they do not specify those conditions in any detail, leaving them up to member countries to determine. A member state is free to adopt more rigorous standards should it wish to do so, as these conditions are considered minimal

[312] *Ibid.*

guidelines. Finally, Part Six covers international co-operation and interoperability in the following paragraphs (20-23):

> 20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.
>
> 21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.
>
> 22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

Moreover, the attached explanatory memorandum[313] regarding international co-operation and interoperability particularly underscores the relevance of the interoperability dimension. It also lists various examples of existing interoperability approaches wherein working platforms have emerged, like the US-EU Safe Harbour framework.[314] Some other relevant references are considered, including the work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region.

2.2.1.2. Privacy law enforcement co-operation

Although the Revised Privacy Guidelines have established a fundamental set of governing principles, it is also important to stress the role of practical international co-operation with respect to privacy enforcement. International law-enforcement co-operation is central to international privacy governance, as it plays a critical role in checking the circumvention of national laws as well as helping in the mitigation of transnational confrontations. Also, enforcement co-operation among states largely depends on convergence in national privacy

[313] *Ibid.*

[314] *Ibid*.

regimes, in particular when a least-controversial approach is adopted by a member state. The OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (the OECD Recommendation on Cross-border Co-operation)[315] is critically important for establishing an effective general framework. By now, most of the OECD Recommendation on Cross-border Co-operation has been incorporated in the Revised Privacy Guidelines. A brief history of the Recommendation may nevertheless be helpful to convey the complex nature of the transborder data flows context, which is the primary focus of the thesis.

Work on the OECD Recommendation on Cross-border Co-operation began in 2006. The main rationale behind the Recommendation was to address the evolving transborder enforcement challenge in the wake of an increase in transborder data-flow activities, as well as to fill the existing gap in legal responses with a forward-looking way.[316] The Recommendation was firmly rooted in the principles enshrined in the OECD Privacy Guidelines of 1981, and clearly acknowledged the implementation challenge, given the variation in domestic approaches. The Recommendation lays down a comprehensive framework for enhanced co-operation among member states' privacy enforcement authorities. One significant outcome of the Recommendation was the emergence of a global privacy enforcement network for facilitating co-operation among national privacy enforcement authorities.[317] The Recommendation provides that:

> Member countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.[318]

---

[315] See OECD Recommendation on Cross-border Co-operations, *supra* note 31.

[316] *Ibid*.

[317] See GPEN, *supra* note 33.

[318] See OECD Recommendation on Cross-border Co-operation, *supra* note 31.

Therefore, one can note a significant expansion of the OECD strategy towards international privacy and personal data governance in the wake of the Revised Privacy Guidelines, 2013. The OECD approaches the issue of privacy alongside security in a broad digital environment that aims to ensure that "the digital economy to continue to serve as a platform for innovation, new sources of economic growth and social development…" as well as to develop policies "to ensure that security and privacy foster economic and social prosperity in an open and interconnected digital world."[319]

2.2.2. EU initiatives on privacy and personal data governance

The EU data protection framework involves two primary governance instruments, the COE 108 and the Data Directive 95/46/EC. The following discussion reflects on the general framework of both the COE 108 and the Data Directive 95/46/EC, with an added focus on international data-flow provisions; it concludes with a brief update on ongoing reforms. The reforms reflect a consensus among the EU Parliament, the Council of Europe and the European Commission on the need for "new data protection rules, establishing a modern and harmonised data protection framework across the EU."[320] These reforms are still a work in progress, but would be applicable within two years of the approval of a new Regulation and Directive from the European Parliament and the Council.

2.2.2.1. Modernization of the COE 108[321]

As Chapter II provides a general overview of the COE 108, this section deals with the Convention's ongoing modernization process.[322] The COE 108 was the first "legally binding

[319] See, OECD, "Information Security and Privacy", online: OECD <http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm>.

[320] These EU institutions reached this agreement on December 15, 2015. See online: European Commission <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>.

[321] See COE 108, *supra* note 18.

[322] See Council of Europe, online: Modernisation of Convention <http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp> [Modernisation of Convention].

international instrument in the data protection field."[323] It imposes on parties the obligation to implement its principles into domestic laws "in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data."[324] The COE 108 entered into force on October 1, 1985.

The Consultative Committee adopted the current modernization proposal on December 18, 2012, at its Strasbourg meeting. The modernization process will conclude with approval by an ad hoc committee on data protection (CAHDATA) consisting of 47 member states as well as 36 other invited countries. The Abridged Report[325] adopted at the end of the first meeting was of a general preparatory nature, and aimed to produce a new working document for the second CAHDATA meeting.

A main focus of the modernization process has been the strengthening of international co-operation, improving competence and enhancing relations among the supervisory authorities, with a specific emphasis on mutual assistance on various fronts, ranging from information sharing to coordination in investigations or interventions. The proposal for the modernization process consists of seven chapters, twenty-seven articles and an additional protocol.[326] Underscoring the importance of the Convention 108, J.Ph. Walter, the Chair of the T-PD, has emphasized that it is "important to have common standards of data protection which are based on international recognized basic principles."[327] He further stated:

> Only internationally agreed standards can provide the legal basis for the free flow of information and data that we urgently need in our globalised world, where

[323] See online: Council of Europe, Data Protection <https://www.coe.int/t/dghl/standardsetting/dataprotection/convention_en.asp>.

[324] *Ibid*.

[325] See Council of Europe, "Abridged Report" (14 November 2013), online: COE <http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA%282013%29RAP01Abr_En.pdf >.

[326] *Ibid.*

[327] See J. Ph. Walter, "The Role of Convention 108 in the International Co-operation", online: COE <http://www.coe.int/t/dghl/standardsetting/DataProtection/Articles/Phaedra%20workshop%20varsovie,%20J-Ph%20W.pdf>.

> fundamental values and essential aspects of private life are at stake, state authorities have a duty to establish an efficient regulatory and enforcement framework of protection, and data protection authorities have the duty to effectively apply this legal framework, notably by enhancing their international co-operation.[328]

Graham Greenleaf (Greenleaf) has examined the role of the modernized Convention from the perspective of its potential globalisation. He argued that the globalisation of the COE 108 is now underway in multiple venues. However, he asserted that the "attraction of globalisation to non-European states depends on the modernisation process establishing a level of data protection that is 'just right.' It can't be too hot (setting standards too high) or too cold (setting standards too low so that it requires exports of personal data to other countries offering little data protection). Modernisation must pass the Goldilocks Test."[329]

In another paper,[330] Greenleaf explored the possibility and desirability of the Council of Europe Data Protection Convention and its Additional Protocol ultimately becoming a global international agreement on data privacy. He argued that for the COE 108 to become globalized, the "Council of Europe will have to settle and publicise appropriate policies on accession that are appropriate, are transparent, and do not reduce European data privacy standards."[331] He vehemently defended the EU's leading role in international data protection by emphasizing that

> Europe has no reason to retreat from its privacy standards developed over forty years. The rest of the world is moving its way, and it should not compromise fundamental standards for the sake of compromise with powerful outliers, particularly the USA and China. Respect for their domestic prerogatives should not

---

[328] *Ibid.*

[329] See Graham Greenleaf, "Modernising Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" (2013) 29.4 Computer L & Sec R, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstractid=2262296#%23>; See also articles on COE 108, online: SSRN <http://www.coe .int/t/dghl/standardsetting/dataprotection/modernisation_en.asp>.

[330] See Graham Greenleaf, "The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108" (2012) 2.2 International Data Privacy Law; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299>.

[331] *Ibid*, Abstract.

> be confused with any need to reduce fundamental aspects of global data privacy standards.[332]

The EU Convention 108 has emerged as one of the strongest and most influential international platforms to shape international privacy governance.

2.2.2.2. EU Data Directive 95/46/EC—ongoing reforms

The EU Data Directive 95/46/EC establishes a strong EU-wide data protection framework. Currently, the process of EU review of the data protection legal framework is underway. The EU Commission is currently reviewing the general EU legal framework with three main policy objectives:

> 1. Modernise the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalisation and the use of new technologies;
>
> 2. Strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a free flow of personal data within the EU and beyond; and
>
> 3. Improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities.[333]

The ongoing legal framework review process involves two legislative proposals. The first involves a "[R]egulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"[334] and the second involves the development of a

---

[332] *Ibid*.

[333] See European Commission, "Reform of the Data Protection Legal Framework", online: European Commission <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>.

[334] See, European Commission, "Regulation of the European Parliament and of the Council on the

"[D]irective of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data."[335]

The main feature of the ongoing review process involves setting up a single set of rules for data protection, designed to remove administrative hassles and save money for businesses. On the Commission's proposal, followed by the European Parliament and Council of Ministers' approval, it will become effective two years after its adoption.[336] Finally, the GDPR entered into force on May 25, 2016 that was based on the recommendation of the EU Commission, the European Parliament and Council agreement on the proposed reforms package, which includes the GDPR and the Data Protection Directive for the police and criminal justice sectors.[337]

After reaching a comprehensive agreement among the EU Parliament, the Commission and the Council, the EU Commission released a new Q&A[338] to provide insight into the nature of the coming reforms. It asserts that the proposed Regulation "updates and modernises the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights." Further, the regulation aims on: "reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards."[339] It also lays down a broad scope with giving

---

Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)", online: European Commission <http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_EN.pdf >.

[335] See online: EUR-Lex <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT>.

[336] See European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Businesses" (25 January 2012) online: European Commission <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>.

[337] See European Commission, "Questions and Answers- Data Protection Reform" (21 December 2015), online: European Commission <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm>.

[338] *Ibid*.

[339] *Ibid*.

people more control and easier access to personal data. It emphasizes that the new rules "are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet."[340] Also, the Regulation establishes new rules, including a right to be forgotten; easier access to one's data; a right to data portability; aright to know when one's data has been hacked; data protection by design and by default; and stronger enforcement of the rules, among others.[341]

2.2.3. APEC initiatives on privacy and personal data governance

This section mainly reflects on the ongoing APEC's efforts on cross-border co-operation measures. In wake of the increasing incidents of transnational confrontations over transborder data flows, the APEC economies launched various initiatives to address some of the emerging challenges, in particular to address transborder enforcement cooperation. The APEC has also expanded the scope of the ongoing measures to other international privacy and data protection regimes, like with the EU to collaborate on transborder data flows issues. The following discussion surveys some of the important measures.

2.2.3.1. Data Privacy Pathfinder initiative[342]

In order to enhance the implementation of the APEC Privacy Framework, the APEC Ministers at Sydney, Australia (2007) meeting established the APEC Data Privacy Pathfinder project (the Pathfinder). The main objective of the Privacy Pathfinder was to "to achieve accountable cross-border flow of personal information within the APEC region."[343] Although, the Pathfinder initiative consisted of multiple projects but the main objective was to develop the

[340] *Ibid*.

[341] *Ibid*.

[342] See APEC, E-Commerce Steering Group, Data Privacy Pathfinder, online: APEC <http://www.apec.org/groups/committee-on-trade-and-investment/electronic-commerce-steering-group.aspx/>.

[343] *Ibid*.

Cross-Border Privacy Rules (CBPR) system. The following outlines the Pathfinder's main objectives:

> 1. Conceptual Framework Principles. Promoting a conceptual framework of principles of how cross-border rules should work across economies, in consultation with the various parties that may be actors in the implementation and enforcement of these rules.
>
> 2. Consultative Process. Promoting the development of consultative processes on how best to include stakeholders including regulators, responsible agencies, lawmaking bodies, industry, third party privacy solutions providers and consumer representatives both in the creation of the rules and processes and in their operational review and optimization.
>
> **3.** Practical Documents. Promoting the development of the practical documents and procedures that underpin cross-border privacy rules such as self-assessment forms, review criteria, recognition/acceptance procedures and dispute resolution mechanisms.
>
> 4. Implementation**.** Exploring ways in which various documents and procedures may be implemented in practice with due consideration to the mandates of the parties involved and the legal frameworks in which they operate, in a manner which is flexible, credible, enforceable, predictable and less bureaucratic.[344]

Greenleaf criticized the Privacy Pathfinder projects as "a generalised version of the US 'Safe Harbor' scheme."[345] He further raised questions on "what standards for data transfers they aim to implement; whether compliance with all of APEC's own Privacy Principles will be required; and how 'Accountability Agents' will be accredited."[346] In overall, the Pathfinder initiative

[344] *Ibid*.

[345] See Greenleaf, "Five Years of the APEC Privacy Framework", *supra* note 40.

[346] *Ibid*.

created a platform that further helped formulation of other major initiatives, like the following CBPR system.

2.2.3.2. Cross Border Privacy Rule system (CBPR)[347]

The CBPR system was developed as a strategic component of the implementation of the APEC Privacy Framework. The main objective of the CBPR system is **"**to protect the privacy of consumer data moving between APEC economies by requiring companies to develop their own internal business rules on cross-border data privacy procedures."[348] The CBPR aims to reduce barriers to information flow, enhance consumer privacy and promote interoperability across regional data privacy regimes.

The main purpose of the CBPR system was to put in place "a simple and transparent system that can be used by organizations for the protection of personal information that moves across the APEC member economies."[349] The CBPR system was based on four elements:

(1) Self-assessment–under this element organizations use tools and guidance to develop and assess their own internal rules and procedures to protect personal information. By doing so, the organization is making a commitment to be held accountable for compliance with its rules and procedures.

(2) Compliance review–this is where the organization's rules and procedures are checked by an appropriate external body (an accountability agent) to make sure that the organization's internal rules and procedures in fact comply with the requirements of the CBPR system.

---

[347] See APEC, "APEC Cross-Border Privacy Rules System", online: APEC <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx> [CBPR].

[348] See APEC, "The Cross Border-border Privacy Rules System: Promoting Consumer Privacy and Economic Growth Across the APEC Region" (5 September 2013), online: APEC <http://www.apec.org/Press/Features/2013/0903_cbpr.aspx> [CBPR Promoting Consumer Privacy].

[349] See CBPR, *supra* note 347.

(3) Recognition/acceptance–organizations that have successfully passed the compliance review process will be placed on a list of participating organizations and will be recognized as such in the APEC region.

Finally, (4) Dispute resolution and enforcement–domestic and cross-border procedures for resolving complaints, including by appropriate regulators.[350]

"By 2011, all projects had been completed and the Cross-Border Privacy Rules (CBPR) system became a reality," added Mr. Harris, Chair of the APEC Cross-Border Joint Oversight Panel.[351] The US and the Mexico officially joined the system in 2012.[352] The key execution instrument adopted for the implementation of the CBPR system involves accountability agents or third parties to verify whether an organization's data privacy policies and practices meet the CBPR requirements. Moreover, on the enforcement side, the "regulators in participating economies are also required to have the ability to take enforcement action under domestic laws and regulations that have the effect of protecting personal data consistent with the CBPR system."[353]

Another significant development was the recognition of the fact that "international group of regulators may work together to assist in data privacy-related investigations or enforcement matters through their participation in the APEC Cross-Border Privacy Enforcement Arrangement (CPEA)"[354] further discussed, in the following section. The Federal Trade Commission (FTC) has been designated as the main enforcement authority. International

[350] *Ibid*.

[351] See CBPR Promoting Consumer Privacy, *supra* note 348.

[352] *Ibid*.

[353] *Ibid*.

[354] *Ibid*.

Business Machine (IBM) was the first US Corporation certified under CBPR system as approved by TRUSTe, the accountability agent.[355] The

2.2.3.3. Cross Border Privacy Enforcement Arrangement (CPEA)[356]

International co-operation over enforcement measures among the national data protection authorities has been one of the central objectives of the APEC Framework. The CPEA lays down a framework for the APEC member co-operation regarding the enforcement of privacy laws. The privacy enforcement authorities of any member countries may participate in the CPEA program. The main goals of the CPEA are:

1. Facilitate information sharing among PE Authorities in APEC economies;

2. Provide mechanisms to promote effective cross-border co-operation between authorities in the enforcement of Privacy Law; and

3. Encourage information sharing and co-operation on privacy investigation and enforcement with PE Authorities outside APEC.[357]

The CPEA clearly spells out a framework for the regional privacy enforcement authorities to co-operate on all aspects of privacy that are implicated into transborder data flows context. This approach generally involves information sharing, enforcement co-operation and investigation collaboration. Further, the CPEA specifically "establishes a process under which participating authorities may contact each other for help with collecting evidence, sharing information on an organisation or matter being investigated, enforcing actions, and transferring

[355] See Donald G. Aplin, "APEC-EU Data Protection Authorities Group Release Data Transfer Interoperability Map" (10 March 2014), online: BNA <http://www.bna.com/apec-eu-data-n17179882705/>.

[356] See APEC, "Cooperation Arrangement for Cross-Border Privacy Enforcement" (28 February 2010), online: APEC <http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf> [CPEA].

[357] *Ibid*.

complaints to another jurisdiction."[358] Unlike the CBPR, which aims to facilitate co-operation among diverse national and regional privacy and data protection regimes[359], the CPEA primarily focuses on the cross-border law enforcement cooperation among the member countries.

2.2.3.4. Inter-regime interoperability—EU-BCR and APEC-CBPR [360]

The Data Privacy Subgroup of the APEC E-Commerce Steering Group established the working groups "to broaden the interest and reduce the costs and efforts involved for private sector companies participating in the APEC process by allowing companies with validation methods of their privacy practices to obtain recognition for their existing processes."[361] The working groups were mandated to "to compare existing economy private sector intake and assessment processes, and also the broader issue of interoperability of privacy systems, to the current APEC Cross-Border Privacy Rules intake documents for applicant organizations and Accountability Agents and the APEC Privacy Principles generally."[362] Further, the DPS created a Working Team with the main objective to "examine the interoperability of the EU and the APEC privacy and data protection regimes."[363] On the EU side, the Article 29 Working Party along with the APEC Working Team developed "a practical tool to map the respective

[358] See e.g. Canada has been accepted as a participant in a new Asia-Pacific Economic Co-operation mechanism for cross-border co-operation on data privacy enforcement. See online: OPC <http://www.priv.gc.ca/media/nr-c/2010/an_100827_e.asp>.

[359] See CBPR Promoting Consumer Privacy, *supra* note 348.

[360] See Electronic Commerce Steering Group, online: APEC <http://apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx> [APEC E-Commerce Steering Group].

[361] See APEC, "Scoping Paper on Privacy System Interoperability" (18 September 2011), online: APEC <mddb.apec.org/documents/2011/ECSG/DPS2/11_ecsg_dps2_013.doc>.

[362] See APEC E-Commerce Steering Groups, *supra* note 360.

[363] *Ibid.*

requirements of the Binding Corporate Rules (BCR) and the CBPR, called the Referential."[364] The Referential marks a new beginning in terms of inter-regime interoperability. Mr. Alhadeff, Vice President of Global Public Policy at Oracle, put it rightly: "[t]he APEC Privacy Framework is drafted at the principles level, but there is huge divergence at the legal and policy implementation level around the world."[365] He further underscored the importance of the ongoing interoperability drive with emphasizing that, "[t]he next step is to bridge these issues and find commonality. APEC's mapping process with the European Union is a part of this step to moving forward."[366]

To conclude, an insight into the ongoing adaptation and modification efforts at the international regimes' is important to understand and explore how the three international regimes are approaching the emerging challenges. The EU with the strong COE 108 and the Data Directive 95/46/EC has launched a massive overhauling process with its primary focus on to streamline the EU wide data protection rules. Again, with the adoption of the Revised Privacy Guidelines of 2013, the OECD still maintained the low threshold while allowing member states to adopt flexible frameworks aimed to attain national regimes' harmonization. Moreover, the APEC has further expanded its efforts through the Privacy Pathfinder project. The APEC projects, like CBPR, CPEA and the ongoing BCR-CBPR interoperability drive have added a new dimension to the international privacy and personal data governance. A significant focus of the ongoing efforts relates to the renewed emphasis on enforcement co-operation and finding ways for inter-regime interoperability. Also, the other striking feature of the ongoing international regimes' initiatives further expanded the prevailing inter-regime co-operation and collaboration towards achievement of common strategies goals.

2.3. Trans-national confrontations over transborder data flows—US-EU context

[364] See for the ongoing joint work between experts from the Article 29 Working Party and from APEC Economies, online: APEC <http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf>.

[365] See CBPR Promoting Consumer Privacy, *supra* note 348.

[366] *Ibid*.

The previous two sections have dealt with the two analytical components—the alliances of data protection authorities with specific focus on the Commissioners' Conference and the three international privacy and data protection regimes. Now, in the following discussion, the third analytical component—the EU-US confrontations over transborder data flows— is analyzed.

Again, it is important to elucidate the analytical rationale of this section. First of all, the transnational confrontations over transborder data flows illuminate a deeper insight into the national and international regimes' convergence-divergence dynamics. That insight is necessary to understand the nature of the implicated states' national interests. Both the US and the EU are leading world economies with advanced privacy and personal data governance frameworks. In terms of the organization of the analysis on this component, two objectives guide the analysis, (1) aims to illuminate the empirical context where various strands of states' national interests are embedded and (2) to develop observations on the EU and US positions further utilized in the conduct of the Chapter V theoretical analysis. Moreover, the following discussion covers the EU-US transborder data flows confrontations context with specific focus on the Safe Harbor agreement.

2.3.1. EU regime on third country data transfers

To reiterate, the EU regime involves two main instruments, the Convention 108 and the Data Directive 95/46/EC. The EU Data Directive 95/46/EC imposes stringent requirements on its member states for the Data Directive's compliance. Other countries around the world have taken heed from the EU Data Directive 95/46/EC's stringent requirements either through *suo motto* adoption of domestic measures or to follow the adequacy assessment process provided under the EU Data Directive 95/46/EC's scheme. The adequacy assessment of the domestic privacy and data protection framework of third country facilities the smooth flow of information between that country and the EU. For example, Canada adopted the domestic privacy and data protection framework[367] aimed to comply with the EU Data Directive 95/46/EC's requirements and approached the EU for its assessment for the adequacy, as prescribed by the Data Directive 95/46/EC. On the other hand, the US confronted the EU on

[367] For example, the Canadian privacy law, *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) is a good illustration.

various issues relating to transborder data transfers while maintaining the national framework that do not meet the EU level of protection.[368] Increasingly, non-EU member countries are voluntarily internalizing the EU model by adopting a wide range of domestic measures.[369]

Central to the EU Data Directive 95/46/EC's provisions over transfer of data to third countries is the requirement of Article 25, which imposes an "adequacy assessment" as a prerequisite before data transfer takes place. Further, a lengthy process for the determination of adequacy assessment is provided under Article 25.6 of the Directive. This process involves a proposal from the Commission followed by an opinion of the group of the national data protection commissioners (Article 29 Working Party) as well as the opinion of the Committee (Article 31) delivered by a qualified majority of the EU member states. It follows a thirty-day right of scrutiny in order to examine whether the Commission has used its executing powers correctly. The European Parliament may, if it considers it appropriate, issue a recommendation. That leads to the adoption of the decision by the College of Commissioners.[370]

The stringent requirements imposed by the EU Data Directive 95/46/EC in relation to transfer of the EU citizens data to third countries has generated confrontations with other countries. The EU-US confrontations are the primary example of transborder data flows conflicts. Since the inception of the Data Directive 95/46/EC, the EU acted both aggressively and strategically to seek compliance of the Data Directive 95/46/EC. It has been successful in ratcheting-up pressure on the US to raise the regulatory threshold on data protection through negotiated agreements, like the Safe Harbor agreement. While in terms of other non-EU member countries, the EU successfully influenced the Canadian and the Australian privacy regimes and

---

[368] See e.g. the US-EU Safe Harbor Agreement reached in 2000. For details, see, Safe Harbor agreement, *supra* note 13.

[369] See e.g. Mexico introduced the omnibus Federal Law on the *Protection of Personal Data Held by Private Parties* in July 2010 primarily drawn on the EU Data Directive 95/46/EC framework in many respects. For details see, Scott Blackmer, "Mexico's New Data Protection Law" (July 28, 2010), online: infolawgroup.com <http://www.infolawgroup.com/2010/07/articles/privacy-law/mexicos-new-data-protection-law/>.

[370] See EU Data Directive 95/46/EC, *supra* note 19. Once the College of Commissioners makes a decision on the adequacy, then personal data can flow from the 27 EU countries and three European Economic Area member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.

has shown no indication of retreat. No doubt, the EU has taken lead in terms of international data protection standard setting. Other countries that are not yet subjected to any direct adequacy assessments like Singapore, Malaysia, Brazil, and Mexico have streamlined their national regimes. Many countries apart from the EU members have approached the EU to seek the adequacy status of their national privacy protection frameworks. The EU Commission has recognized the following countries' privacy frameworks as adequate: Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US Department of Commerce's Safe Harbour Privacy Principles.[371] The following section examines some specific instances of the EU-US confrontations over transborder data flows.

2.3.2. EU-US confrontations over transborder data flows

In response to the EU adopted GDPR initiative, Colin Bennett argued that, "the heightened rhetoric on proposed Draft EU Regulation's implications over the EU-US relations as simplistic and misleading."[372] He contended that the same line of arguments were raised when the EU Data Directive 95/46/EC was enunciated in 1995 and that issue was resolved through transatlantic negotiation resulted in the Safe Harbor agreement. Rather, the thesis takes strong reservation on Bennett's position on the EU-US confrontations and argues that the divide between the EU and the US over privacy governance is not simplistic; rather, it is complex and deeply political. This argument is further developed in Chapter VI. In the following discussion, the thesis reflects on the ongoing EU-US confrontations. First, a brief outline of the EU and the US general approaches on privacy and data protection is presented. Then, the context of the Safe Harbor agreement is elucidated. Further, additional insights into other issue areas, like the PNR and recently concluded the Umbrella Agreement and the Privacy Shield arrangements are highlighted.

---

[371] See, "Commission Decisions on the Adequacy of the Data Protection of Personal Data in Third Countries", online: European Commission <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> [European Commission's Decisions on Adequacy].

[372] See Colin Bennett, "The Geo-Politics of Personal Data", (December 14, 2012), online: Harvard International Review <http://hir.harvard.edu/archives/3016>.

The US and the EU approaches to privacy and data protection differs on various fronts. Though, the US and some of the EU member countries are signatories to the OECD Privacy Guidelines, they diametrically diverge on domestic legal and regulatory frameworks. The EU member countries have to put in place a comprehensive domestic legal framework to protect personal data to meet the requirements of the Data Directive 95/46/EC. The EU data protection framework requires a comprehensive national legal regime in each of the member states that generally applicable to both public and private sectors activities dealing with personal data. On the other hand, the US has a medley of scattered patchwork of sectoral and self-regulatory form of regulatory approach. The US has developed separate governing frameworks for the public and the private sectors. In terms of value attachment, the EU recognizes the right to privacy as a human right generally recognized into national constitutions while on the other hand the US approaches it primarily from a consumer rights perspective. The following description provided by the US Departments of Commerce (DOC) captures the very essence of both the EU and the US approaches.

> While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The EU, however, relies on comprehensive legislation that requires, among other things, the creation of independent government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin.[373]

2.3.2.1. Safe Harbor agreement[374]

The Safe Harbor agreement between the US and the EU was concluded in 2000 after two years of heated negotiations. Generally speaking, the following three considerations underpin the

[373] See The US Department of Commerce (DOC) provided overview on the Safe Harbor, online: DOC <http://export.gov/safeharbor/eu/eg_main_018476.asp>.

[374] *Ibid.*

emergence of the Safe Harbor agreement: first, to respond to the EU Data Directive 95/46/EC prescribed third country adequacy requirements; second, to address the potential for adverse implications of the EU Data Directive 95/46/EC on the US businesses; and third, to minimize the sovereign interference or extraterritorial reach of the EU Data Directive 95/46/EC while, at the same time, protecting national interests without committing to the introduction of comprehensive national framework.

The debate preceding the conclusion of the Safe Harbor negotiations evolved all along the construction of the EU Directive 95/46/EC itself because the stakeholders on both side of the Atlantic were keenly following the developments at the EU. During the development of the Data Directive 95/46/EC, the EU policy-makers were under tremendous pressure to address the controversial Data Directive 95/46/EC's provision (Article 25) on transfer of personal data of the EU citizens to the US, as major US corporations were involved in extensive data transfer activities through transatlantic trade and commerce. The fear of a weak existing US national regime along with the higher threshold of the EU Data Directive 95/46/EC created ripple effects among policy makers and legislators. For the EU policy makers, the challenge was to ensure the Data Directive 95/46/EC's compliance while for the US policy makers the challenge was how to address the EU concerns while protecting national interests at the same time. From the very beginning, it was clear that the EU was relentless in its defense whereas the US was unwilling to transplant the EU model into its domestic framework.

Under the Data Directive 95/46/EC's mandate, the EU Commission is vested with power to launch negotiation with a third country to decide whether a third country's regime meets the EU Data Directive 95/46/EC's prescribed "adequacy" threshold. Therefore, under the Directive's mandate, John Mogg, then Director General for the Internal Market, launched negotiations with the US counterpart, Ambassador David Aaron, the Undersecretary for International Trade in the Department of Commerce. The initial stance of both parties were marred by the heated and controversial posturing as the "European Union maintained that it was interested only in legislation drafted to provide adequate protection to the data of European citizens which had been exported, while the US sought to postpone the

implementation of the Directive, and to gain a recognition of adequacy for the US system as it then stood."[375]

Nonetheless, the compromising position emerged with both the US and the EU departing from the initial posturing with a central idea to lower down the EU Data Directive 95/46/EC's adequacy threshold to bring in the US businesses within its prescribed requirements. On the other hand, the US agreed on to put in place a new arrangement enshrined in the Safe Harbor agreement. On the EU side, after reviewing the proposed principles, many amendments along with appended FAQ were developed. Ultimately, after lengthy deliberations and negotiations both parties signed the Safe Harbor agreement in 2002. In terms of goals it is provided:

> The U.S.-EU Safe Harbor Framework, which was approved by the EU in 2000, is an important way for U.S. organizations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU member state authorities under EU member state privacy laws. Self-certifying to the U.S.-EU Safe Harbor Framework will ensure that EU organizations know that your organization provides "adequate" privacy protection, as defined by the Directive.[376]

On substance and procedural matters, the Safe Harbor involves seven principles, namely: notice, choice, onward transfer (transfers to third parties), access, security, data integrity, and enforcement.[377] On enforcement both the private sector and the US government are involved. It has prescribed a lengthy dispute resolution process along with verification and remedy recourses. The Safe Harbor agreement brought the scope of self-regulatory measures in compliance with the EU Data Directive 95/46/EC. Moreover, the Safe Harbor agreement stipulates conditions for any US government organization, like FTC to act as an enforcement authority.

---

[375] See Henry Farrell, "Negotiating Privacy across Arenas– The EU-US 'Safe Harbor' Discussions" in Adrienne Hèritier, ed, *Common Goods: Reinventing European and International Governance* (Lanham, Maryland: Rowman and Littlefield, 2002) at 107.

[376] *Ibid.*

[377] See Safe Harbor agreement, *supra* note 13.

The Safe Harbor agreement has provided an alternative platform to avoid the trans-Atlantic trade and commerce disruptions. The US DOC maintains a list of companies participating in the Safe Harbor program.[378] However, the Safe Harbor has been subject to extensive criticism including lack of transparency and weak enforcement process. The EU has been very skeptical about the Safe Harbor success from the very beginning; it has been embroiled in various controversies on how to ensure the working of the Safe Harbor agreement. The EU has assessed the effectiveness of the Safe Harbor framework from time to time.[379] The EU Parliament passed a resolution to suspend the Safe Harbor program in the wake of the reports of the US massive surveillance program.[380] The major challenge to the Safe Harbor agreement emerged in wake of the ECJ decision in *Schrems* case filed against the Ireland's Office of the Data Protection Commissioner, where the ECJ dealt with the question: Does the Safe Harbor program adequately protect the rights of EU citizens when "compliant" companies are known to share EU citizen data with U.S. intelligence bodies, such as the NSA?[381] Finally, the ECJ declared the Safe Harbor agreement as invalid in the *Schrems* decision, which led to the

---

[378] *Ibid.* See the Safe Harbor list, online: export.gov <https://safeharbor.export.gov/list.aspx>.

[379] For additional EU documents on the Safe Harbor agreement, the opinions and reports of the Article 29 Working Party (Working Party) are critical. The Working Party decision can be found online: Opinions and recommendations <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>. Also, the European Commission has prepared various reports and working documents on the Safe Harbor agreement including, The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. The European Commission, Decisions on Adequacy, online: European Commission <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/sec-2002-196_en.pdf>; The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (2004); online: European Commission <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/sec-2004-1323_en.pdf>; see also European Commission's Decisions on Adequacy, *supra* note 371.

[380] See EPIC, "European Parliament: Suspend Safe Harbor, Data Transfers to United States" (12 March 2014), online: EPIC <http://epic.org/2014/03/european-parliament-suspend-sa.html>.

[381] See Sam Pfeifle, "ECJ Hears Safe Harbor Arguments" (24 March 2015), online: IAPP <https://iapp.org/news/a/ecj-hears-safe-harbor-arguments/>; see also *Schrems* decision, *supra* note 8.

adoption of the recently concluded the EU-US Privacy Shield arrangement, discussed in details in the following section that deals with the EU-US Privacy Shield.

2.3.2.2. Air passenger name record and data transfer on terrorist finance tracking program

The other major initiative was launched by the EU with regard to air passenger name record (PNR) data transfer and Terrorist Finance Tracking Program (TFTP)[382] agreement where the EU negotiated with the US, Canada, and Australia various agreements.[383] These bi-lateral agreements covered the PNR transfers of all air travellers during tickets reservation and booking aimed to control serious crimes by law enforcement authorities. The main EU objective was to ensure that such transfers "must be governed by a bilateral agreement that provides for a high level of personal data protection."[384]

The interesting development with regard to the EU-Canada PNR Agreement would be the forthcoming ECJ opinion on that agreement. On November 25, 2014 the MEPs referred the EU-Canada PNR Agreement to the ECJ in order to make ensure "whether it is in line with the EU treaties and Charter of Fundamental Rights,"[385] This reference to the ECJ will have implication on the EU PNR transfer agreements with other countries as it has temporarily

[382] See Transfer of Air Passenger Name Record (PNR) Data and Terrorist Finance Tracking Program (TFTP), online: European Commission <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp/index_en.htm> [TFTP].

[383] For the list of the EU agreements on PNR and Terrorist Finance Tracking Program (TFTP), see online: European Commission <http://ec.europa.eu/justice/data-protection/international-transfers/pnr-tftp/pnr-and-tftp_en.htm> [European Commission on PNR-TFTP].

[384] *Ibid*.

[385] See European Parliament, News Release, "MEPs refer EU-Canada Air Passenger Data Deal to the EU Court of Justice" (25 November 2014), online: European Parliament <http://www.europarl.europa.eu/news/en/news-room/20141121IPR79818/MEPs-refer-EU-Canada-air-passenger-data-deal-to-the-EU-Court-of-Justice>.

suspended the ongoing negotiations with Mexico.[386] The following paragraph encapsulates the prospective implications of the ECJ opinion:

> Once the European Court of Justice has issued its opinion on the draft PNR Agreement with Canada, and based on the Court's conclusions, the Commission will finalise its work on legally sound and sustainable solutions to exchange PNR data with third countries, including by considering a model agreement setting out the requirements third countries have to meet to be able to receive PNR data from the EU.[387]

Thus, the ECJ opinion on the PNR will have considerable implications and may result in revision of the existing EU agreements on the PNR transfers. Now, with the US, the EU signed an additional agreement on the Terrorist Finance Tracking Programme regulating the transfer of financial transactions data.[388] The TFTP agreement aim to "strengthens data protection guarantees relating to transparency, rights of access, rectification and erasure of inaccurate data… guarantees non-discriminatory rights of administrative redress and… ensures… the right to seek in the U.S. judicial redress for any adverse administrative action."[389] From the analytical objective this brief reflection on these measures, in particular the submission of the EU-Canada PNR agreement to the ECJ opinion, sheds light on a consistently evolving EU data protection regime.

2.3.2.3. US-EU Umbrella Agreement

---

[386] See European Parliament, Parliamentary Questions (5 October 2015), online: European Parliament <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2015-009612&language=EN> (as noted, "the Commission has advised Mexican authorities that the negotiations with Mexico cannot be finalised until the European Court of Justice has delivered its opinion on the Draft EU-Canada PNR Agreement").

[387] See European Commission, "Passenger Name Record", online: European Commission <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr/index_en.htm>

[388] See TFTP, *supra* note 382.

[389] *Ibid*.

On September 8, 2015, the EU and the US signed a very important agreement called the "Umbrella Agreement."[390] The negotiations were aimed to protect personal data transferred between the EU and the U.S. for law enforcement purposes. This includes cases in which personal data is sent from the EU to the U.S. for the prevention, detection, investigation and prosecution of criminal offences, including terrorism."[391] The major push for the Umbrella Agreement negotiations came from a decision of Justice Ministers (December 3, 2010), mandating the Commission to achieve the following goals:

1. Provides for a coherent and harmonised set of data protection standards including essential principles such as proportionality, data minimisation, minimal retention periods and purpose limitation;

2. Contains all the necessary data protection standards in line with the EU's existing data protection rules, such as enforceable rights of individuals, administrative and judicial redress or a non-discrimination clause;

3. Ensures the effective application of data protection standards and their control by independent public authorities.[392]

In a recent visit to Washington DC, a delegation of members of the European Parliament's (MEP) civil liberty committee stressed that the US should provide "equal enforceable rights to effective judicial redress for EU citizens when personal data is transferred for law enforcement purposes."[393] Further, in a meeting with the US Trade Representative's Office the EU

[390] See European Commission, "Factsheet EU-US Negotiations on Data Protection" (June 2014), online: statewatch.org <http://www.statewatch.org/news/2014/jun/eu-usa-dp-deal-pnr-factsheet.pdf>.

[391] *Ibid*.

[392] See European Commission, "European Commission Ready to Start Talks with US on Personal Data Agreement to Fight Terrorism or Crime" (3 December 2010), online: European Commission <http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm>.

[393] See European Parliament, "Civil liberties MEPs Make Case for Data Protection During Washington Visit" (24 March 2015), online: European Parliament News <http://www.europarl.europa.eu/news/en/news-room/content/20150320STO36310/html/Civil-liberties-MEPs-make-case-for-data-protection-during-Washington-visit>.

delegation of MEPs emphasized that the data protection should remain outside the scope of the Transatlantic Trade and Investment Partnership (TTIP) negotiations with stressing that the EU's data protection framework must remain in place.[394] Finally, at the conclusion of the Umbrella Agreement, the EU Commission issued the statement that underscores that:

> Once in force, this agreement will guarantee a high level of protection of all personal data when transferred between law enforcement authorities across the Atlantic. It will in particular guarantee that all EU citizens have the right to enforce their data protection rights in US courts…[395]

A strong critical statement of the Vice-President, Viviane Reding on the TTIP reflects the acrimonious confrontations on the ongoing negotiations. She asserted, "[i] warn against bringing data protection to the trade talks. Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable."[396] She further emphasized, "[o]nce a single, coherent set of rules is in place in Europe, we will expect the same from the US."[397]

Mark Rotenberg, the Electronic Privacy Information Centre (EPIC) president, has recommended that in order to avoid the EU-US confrontations over transborder data flows, the US, *inter alia*, should update its privacy laws to be more closely align with European policy. Furthermore, he argued that the US should do more to support a viable international framework

---

[394] *Ibid*.

[395] See European Commission, Press Release Database, "Statement by EU Commissioner Věra Jourová on the Finalisation of the EU-US Negotiations on the Data Protection 'Umbrella Agreement'" (8 September 2015), online: European Commission < http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm>.

[396] See e.g. the European Commission, Press Release Database, Viviane Reding, "Towards a more Dynamic Transatlantic Area of Growth and Investment" (29 October 2013), online: European Commission <http://europa.eu/rapid/press-release_SPEECH-13-867_en.htm/> [Viviane Reding, "Dynamic Transatlantic Growth"].

[397] *Ibid.*

for privacy protection by ratifying the COE 108.[398] For a privacy advocate, these arguments appear sound yet fall short on the pragmatic assessment. For example, this view does not explain: how the US can build on the COE 108? What would be the implications of such policy alignment with the EU on the US's commercial and security interests? The following words of Viviane Reding are quite instructive to sum up the EU-US divide over privacy and data protection:

> The existing scheme has been criticised by European industry and questioned by European citizens: they say it is little more than a patch providing a veil of legitimacy for the US firms using it. Data flows between the EU and the US must therefore rely on solid legal foundations on both sides... We expect the US to quickly set its side of the bridge. It is better to have steady footing on a bridge than to worry about the tide in a 'Safe' or, after all, not so 'Safe' harbour.[399]

Finally, the US Congress passed the *Judicial Redress Act* recently, which has become law after signed by the US President Barack Obama on February 24, 2016. However, the EU side has yet to take necessary steps to formalize the EU-US Umbrella Agreement.

2.3.2.4. US-EU Privacy Shield arrangement—ECJ's *Schrems* decision

The recent ECJ decision in *Schrems*[400] case is probably been the most important event with serious implication on trans-Atlantic data transfer. The decision invalidated the US-EU Safe Harbor agreement and pushed both the EU and the US authorities to devise alternative mechanism. One such major consequence is the recently concluded the EU-US Privacy Shield arrangement.

---

[398] For additional insights, see Mark Rotenberg, "On International Privacy: A Path Forward for the US and Europe" (15 June 2014), online: Harvard International Review <http://hir.harvard.edu/on-international-privacy-a-path-forward-for-the-us-and-europe/>.

[399] See Viviane Reding, "Dynamic Transatlantic Growth", *supra* note 396.

[400] See *Schrems* decision, *supra* note 8.

To reflect back, the *Schrems* case begins with Maximillian Schrems, an Austrian privacy activist[401] challenged to the Facebook for privacy violation protected under the European privacy laws. Schrems filed a complaint against Facebook Ireland Ltd. with the Irish Data Protection Commissioner, who rejected the complaint on the ground that the European Commission has determined the Safe Harbor agreement as adequate[402] to under the Data Directive 95/46/EC's requirements. Then, *Schrems* filed the application for judicial review in the Irish High Court, which was adjourned pending the reference to the ECJ. Finally, the ECJ delivered its decision on October 6, 2015 with main ruling declaring the Safe Harbor agreement as invalid[403] and also rejecting the notion that the "existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to the national supervisory authorities."[404] Further, the ECJ press release concluded with the assertion that:

> The Court holds that the Commission did not have competence to restrict the national supervisory authorities' powers in that way. For all those reasons, the Court declares the Safe Harbour Decision invalid. This judgment has the consequence that the Irish supervisory authority is required to examine Mr. Schrems' complaint with all due diligence…[405]

The ECJ decision pushed both the EU and the US sides to devise strategies and develop new approach to address the ECJ ruling requirements, which led to the conclusion of the EU-US Privacy Shield arrangement. Although, the thesis' main research focus is on the Safe Harbor

---

[401] See Wikipedia, online: Max Schrems <https://en.wikipedia.org/wiki/Max_Schrems> [Schrems Webpage].

[402] See the European Commission's decision of the adequacy of the Safe Harbor agreement (26 July 2000), online: European Commission <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>.

[403] See the Court of Justice of the European Union, Press Release, "The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid" (6 October 2015), online: ECJ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.

[404] *Ibid*.

[405] *Ibid*.

agreement, but in wake of the implications of the ECJ's *Schrems* decision on the Safe Harbor agreement, both the EU and the US sides has taken up the matter seriously. Both, the EU-US has already agreed on the EU-US Umbrella Agreement for data transfers for law enforcement purposes, the EU-US Privacy Shield arrangement has formulated a new framework that will further govern the commercial data exchange, which has been previously governed by the Safe Harbor agreement. Also, it is important to underscore that the thesis has very limited opportunity to engage in a deeper analysis of the evolving EU-US Privacy Shield arrangement, as its detailed institutional and implementation design has yet to emerge; still, in the following a brief introduction to the EU-US Privacy Shield is presented to inform the readers on the ongoing efforts.

On February 29, 2016 the European Commission released the legal text that would put in place the EU-US Privacy Shield aimed to restore trust in transatlantic data flows.[406] The EU-US Privacy Shield is one of the triad reforms that the EU Commission has launched to overhaul the EU data protection framework, which includes new EU data protection rules, the EU-US Umbrella Agreement and the EU-US Privacy Shield. The EU-US Umbrella Agreement addresses the issue of transatlantic data transfer in law enforcement matters whereas the EU-US Privacy Shield governs the commercial data exchange. The US government has agreed with the EU Commission to publish the EU-US Privacy Shield principles in the U.S. Federal Register as well as to enforce the agreement. The following observation made by the EU Commissioner Jourova succinctly captures the essence and objectives of the reached EU-US arrangement.

> The EU-U.S. Privacy Shield is a strong new framework, based on robust enforcement and monitoring, easier redress for individuals and, for the first time, written assurance from our U.S. partners on the limitations and safeguards regarding access to data by public authorities on national security grounds. Also, now that President Obama has signed the Judicial Redress Act granting EU citizens the right to enforce data protection rights in U.S. courts, we will shortly propose the signature

[406] See European Commission, Press Release, "Restoring Trust in Transatlantic Data Flows through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield" (29 February 2016), online: European Commission <http://europa.eu/rapid/press-release_IP-16-433_en.htm> [European Commission, "Restoring Trust"].

> of the EU-U.S. Umbrella Agreement ensuring safeguards for the transfer of data for law enforcement purposes. These strong safeguards enable Europe and America to restore trust in transatlantic data flows.[407]

One of fundamental objective of the EU-US Privacy Shield arrangement is to meet the requirements set by the European Court of Justice (ECJ) in *Schrems* case[408] as well as to address the concerns that have emerged in wake of the massive US surveillance program. The EU-US Privacy Shield is designed to guarantee strong obligations on companies and robust enforcement, clear safeguards and transparency obligations on US government access, effective protection of EU citizens' rights with several redress possibilities, and annual joint review mechanism.[409]

To reflect briefly on the EU-US Privacy Shield framework's comparison with the Safe Harbor agreement, the major changes involve three main aspects: "(1) changes to the substantive Privacy Principles with which certifying organizations must comply; (2) changes to the administration and supervision of the framework; and (3) explication of limitations on U.S. government access to data transferred under the Privacy Shield."[410] Given, the extensive changes the EU-US Privacy Shield have received criticism from NGO's, like the EPIC. Speaking to the EU Parliament, Mark Rotenberg urged the EU Commission to "to rewrite the Privacy Shield, saying it fails to safeguard human rights and does not reflect changes in US law as required by the Schrems decision."[411]

To conclude, this chapter begins with highlighting the nature of the emerging challenges to

---

[407] *Ibid*. The European Commissioner Jourova statement quoted in the press release.

[408] See *Schrems* decision, *supra* note 8.

[409] See European Commission, "Restoring Trust", *supra* note 406.

[410] For further discussion on this aspect, see Hogan Lovells, "Inside the New and Improved EU-U.S. Data Transfer Framework" (7 March 2016), online: ehoganlovells.com <http://ehoganlovells.com/rv/ff0025ef4a7ac6bd207d455e8947aff69d7b728e>.

[411] See EPIC, "EPIC's Rotenberg Urges European Parliament to Condition 'Privacy Shield' on End of 702 Surveillance" (17 March 2016), online: EPIC <https://epic.org/2016/03/epics-rotenberg-urges-european.html>.

privacy and data protection by placing the issue in global information society context. Then, it expands on the ongoing international efforts to address the emerging challenges at three international arenas. Further, the EU-US confrontations are analyzed as an illustration of the trans-national confrontations over transborder data flows. In overall, the above discussion aims to take stock of the *status quo* of the international privacy and personal data governance. The following chapter examines the role of data protection authorities in international privacy and personal data governance, from theoretical perspective.

Chapter IV. Role of data protection authorities in privacy and personal data governance

This chapter examines the role of the data protection authorities (DPA) in privacy and personal data governance. Though the main focus of the thesis is on the Commissioners' Conference, this chapter reflects more broadly on emerging alliances of other data protection authorities. From a theoretical perspective, it draws on studies of the role and activities of transgovernmental networks in global governance.

Before further analysis, it is important to reflect back on the underlying rationale for including the data protection authorities. The thesis' analysis began with a set of observations drawn from the ongoing initiatives of the Commissioners' Conference, reflected in its adopted resolutions, as discussed at length in Chapter III. The Commissioners' Conference has taken up a leading position in privacy governance, with its strong commitment to addressing the emerging challenges surrounding the issue of privacy and data protection. It was also seen in Chapter III how the nature and scope of these emerging challenges are informed by the technological, economic and security contexts of personal data, along with their implications for existing privacy and personal data governance frameworks. Chapter III additionally surveyed ongoing measures to address these challenges in each of the three main international regimes. Now, this and the following chapters expand on that analysis from a theoretical perspective, in order to explore the question of the feasibility of developing a new regime.

With respect to the Commissioners' Conference, this analysis focuses on identifying, assessing and explaining its initiatives and strategies from a theoretical perspective. The analysis has four aspects: first, it provides a general introduction to the notion of data protection authorities; second, it situates the data protection authorities in the broader theoretical literature on transgovernmental networks; third, it examines the role of data protection authorities in privacy and personal data governance through the lens of these theoretical perspectives; and fourth, it assesses the implications of this analysis for the research question and for the alternative strategies that the thesis recommends.

1. Data protection authorities

It is important to consider data protection authorities from two distinct analytical perspectives: (1) the general notion of a DPA in a national context, and (2) the emergence of DPA alliances at the international level. From the national perspective, a data protection authority is primarily a national privacy regulator, privacy commissioner or data protection authority created under a certain form of governing statutory arrangement. Many terms are used to designate this somewhat singular conception.[412]

A common feature shared by almost all of the data protection authorities is that they are primarily national regulatory bodies created by a governing legislation. A DPA's function generally involves investigative, enforcement, compliance, and consultation powers.[413] Typically, a privacy enforcement authority investigates complaints or takes *suo motto* measures in the public interest, engages in statutory-jurisdictional interpretations, initiates enforcement measures and executes statutorily prescribed policy objectives. Also, a data protection authority's office publishes various reports and takes part in the broad policy dialogue affecting privacy matters. Thus, a PEA at the national level executes dual functions: the jurisdictional and the policy-related roles. Under the jurisdictional role, a PEA primarily interprets a governing statute to establish its own jurisdiction over a subject matter. Because of that authority, it becomes a powerful national administrative body and often receives judicial deference based on its expert capacity. However, in the policy dimension, a PEA is generally assigned wider latitude to implement government policies through discretionary powers. Further, Raab has recognized some common objectives shared by the DPAs, which provide a fundamental framework for their engagements, like "a long-established set of data protection principles; an understanding of the available regulatory instruments and their combinations;

---

[412] Generally, national laws on privacy and data protection establish an office of national enforcement authority to enforce and implement the statutorily prescribed rights. For example, the Canadian privacy law, *PIPEDA*, establishes responsibilities for the Privacy Commissioner of Canada. See online: OPC, Acts and Regulations <shttps://www.priv.gc.ca/leg_c/r_o_p_e.asp> [*PIPEDA*]; see Bennett & Raab, "Governance of Privacy", *supra* note 5 (the authors have listed a wide range of roles and responsibilities of data supervisory agencies, with illustrations from many countries like Sweden, Germany, the UK, etc.) at 133-43; see Chapter III, above discussion on Commissioners' Conference.

[413] See Bennett & Raab, "Governance of Privacy", *ibid* (according to the authors, "Commissioners act, variously, as ombudsman, auditors, consultants, educators, negotiators, policy advisors, and enforcers") at 134.

agreement on the issues generated by contemporary surveillance and privacy invasion; and the repertory of roles and tasks that they have to undertake to protect privacy and limit surveillance."[414]

In international privacy instruments, both terms, "data protection authorities" and "privacy enforcement authorities", are used. For example, the EU data protection framework has used the term "data protection authorities" whereas the APEC Privacy Framework has used the term "privacy enforcement authorities". The first formal alliance of data protection authorities was established by EU Data Directive 95/46/EC under Article 29's provisions for the creation of the Working Party.[415] It is composed of a supervisory authority representative from each member country, a representative of the authority or authorities established for the Community institutions[416] and bodies, and a representative of the Commission.[417] The Working Party acts as an independent advisory body, with an elected chairman for two years, takes decisions by simple majority, and makes its own rules of procedure.[418] Further, Article 30 of EU Data Directive 95/46/EC lists the main responsibilities of the Working Party, which include: application of national measures in compliance with EU Data Directive 95/46/EC; delivery of opinions to the Commission on the level of protection in the Community and in third countries; advising the Commission on proposed amendments to EU Data Directive 95/46/EC; and submission of an annual report to the Commission, the European Parliament and the Council.[419]

---

[414] See Charles D. Raab, "Information Privacy: Networks of Regulation at the Sub-global Level" (2010) 1:3 Global Policy Journal 291 at 292.

[415] See EU Data Directive 95/46/EC, *supra* note 19.

[416] The European Data Protection Supervisor is the office created in 2001 with "the responsibility… that all EU institutions and bodies respect people's right to privacy when processing their personal data." See online: European Data Protection Supervisor <http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm>.

[417] See EU Data Directive 95/46/EC, *supra* note 19, Article 29 (2).

[418] *Ibid*, Article 29 (3-6).

[419] *Ibid*, Article 30.

Another major international platform for DPAs emerged in the form of an annual gathering of the privacy commissioners, which was initially a Western European based alliance. The privacy advocates' alliance further expanded to include a majority of the Working Party members and now involves other countries' authorities, like the Canadian OPC and the US FTC. Apart from the Commissioners' Conference, other PEA alliances are on the horizon, like the Francophone Association of Data Protection Authorities (AFAPDP),[420] the Ibero-American Data Protection Network (RIPD),[421] the International Working Group on Data Protection in Telecommunications (IWGDPT),[422] the Central and Eastern European Data Protection Authorities (CEEDPA),[423] and the Asia Pacific Privacy Authorities (APPA).[424] The emergence of the Global Privacy Enforcement Network (GPEN)[425] is another example in the context of the OECD privacy framework.

Generally, international alliances of data protection authorities are either a creation of an umbrella institutional framework, like the Working Party created by EU Data Directive 95/46/EC, are part of a broad organization's institutional objective delivery scheme, like the GPEN, or have emerged on a *suo motto* basis to form an international network, like the Commissioners' Conference. For her part, Slaughter has identified three main sources of the

[420] The International Organization of la Francophone member countries formed the association of authorities for personal data protection of the French-speaking countries in 2007. See online: afapdp.org <http://www.afapdp.org>.

[421] The Ibero-American Data Protection Network involves 22 member data protection authorities. See online: redipd.org <http://www.redipd.org/index-iden-idphp.php>.

[422] The International Working Group on Data Protection in Telecommunications (IWGDPT), founded in 1983 under the framework of the International Conference of Data Protection and Privacy Commissioners, headed and chaired by the Berlin Commissioner for Data Protection. See online: datenschutz <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>.

[423] The Asia Pacific Privacy Authorities (APPA) came into existence in 1992 as a forum for privacy authorities in the Asia Pacific Region. See online: APPA <http://www.appaforum.org>.

[424] The APPA is the principal forum for privacy authorities in the APEC Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. See online: APPA <http://www.appaforum.org/members/index.html>.

[425] See GPEN, *supra* note 33.

emergence of transgovernmental networks, namely: 1) establishment by an international organization, 2) creation through a state-negotiated executive agreement and 3) "spontaneous" development outside a formal framework to address a common problem.[426] The scope of the authority of the DPA alliance largely depends on three factors. First, its affiliation with international institutions or organizations—that is, whether it was created under the auspices of an umbrella organization or institution. Second, whether it emerged as a voluntary alliance of national counterparts. And third, whether it is promoted by a state and/or states in order to address a specific common transnational issue. This general scheme accounts for the emergence of various forms of international alliances, ranging from the International Judicial Institution to Basel Committee on Banking Supervision to Financial Action Task Force.[427]

2. Data protection authorities vis-à-vis transgovernmental networks

Despite the fact that the data protection authorities are national regulatory agencies primarily endowed with statutorily prescribed roles and responsibilities, they have strategically expanded their policy roles so as to stretch beyond national borders. The data protection authorities have formed international alliances with their counterparts from other states, with the aim of playing an active role in global privacy and personal data governance. The recent emergence of many DPA alliances has positioned them with other recognized international alliances of non-state actors, like alliances of transgovernmental networks. How to examine the role of data protection authorities' networks in global privacy and personal data governance? In order to address this question, the thesis draws on existing theoretical literature on non-state actors and global governance, in particular the literature on transgovernmental networks.

In order to organize the analysis of data protection authorities, the thesis relies heavily on the scholarly work of the following scholars—Anne-Marie Slaughter (Slaughter),[428] Charles D.

[426] See Anne-Marie Slaughter, "The Accountability of Government Networks" (2001) 8:1 Ind J Global Legal Stud 353 [Slaughter, "Accountability of Government Networks"]. This categorization adapts Slaughter's typology described as: (1) "Government Networks within International Organizations"; (2) "Government Networks within the Framework of an Executive Agreement"; and (3) "Spontaneous Government Networks", at 355-59.

[427] See Slaughter, "A New World Order", *supra* note 24 at 16.

[428] See Anne-Marie Slaughter & Thomas N. Hale, "Transgovernmental Networks" in Mark Bevir, ed, *Sage Handbook of Governance* (London: SAGE Publications, 2011) at 324 [Slaughter & Hale}; Ann-

Raab (Raab),[429] Abraham L. Newman (Newman),[430] Graham Greenleaf (Greenleaf),[431] and Colin J. Bennett.[432] Slaughter, along with other scholars, has generated a rich literature on transgovernmental networks, whereas Raab, Newman, Greenleaf, and Bennett have examined the data protection authorities in diverse contexts, drawing on theoretical perspectives from

---

Marie Slaughter & David Zaring, "Networking Goes International: An Update" (2006) 2 Annual Review of Law and Social Science 211 [Slaughter & Zaring]; Ann-Marie Slaughter, "Global Government Networks, Global Information Agencies, and Disaggregated Democracy" (2003) 24 Mich J Int'l L 1041 [Slaughter, "Global Government Networks"]; ———"Agencies on the Loose? Holding Government Networks Accountable" in George A. Bermann, Matthias Herdegen & Peter Lindseth, eds, *Transatlantic Regulatory Co-operation* (Oxford: Oxford University Press, 2001) [Slaughter, "Agencies on the Loose"];———"Disaggregated Sovereignty: Toward the Public Accountability of Global Government Networks" (2004) 38:2 Government and Opposition 159 [Slaughter, "Disaggregated Sovereignty"].

[429] See Raab & Koops, *supra* note 99.

[430] See Abraham L. Newman & Henry D. Farrell, "The New Politics of Interdependence: Cross-National Layering in Trans-atlantics Regulatory Disputes" (2015) 48:4 Comparative Political Studies 497 [Newman & Farrell]; Abraham L. Newman & David Bach, "The European Union as a Hardening Agent: Soft law and the Diffusion of Financial Regulation" (2014) 21:3 Journal of European Public Policy 430 [Newman & Bach, "Hardening Agent"]; ———"Transgovernmental Networks and Domestic Policy Convergence: Evidence from Insider Trading Regulation" (2010) 64:3 International Organization 505 [Newman & Bach, "Transgovernmental Networks"]; Abraham L. Newman & Burkard Eberlein, "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union" (2008) 21:1 Governance 25 [Newman & Eberlein]; Abraham L. Newman, "Watching the Watchers: Transgovernmental Implementation of Data Privacy Policy in Europe" (2011) 13:2 Journal of Comparative Policy Analysis 181 [Newman, "Watching the Watchers"]; ———"Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive" (2008) 62:1 International Organization 103 [Newman, "Transnational Civil Liberties"]; ———"Creating Privacy: The International Politics of Personal Information" thesis Doctor of Philosophy in Political Science University of California, Berkeley, 2005 [Newman, "Creating Privacy"].

[431] See Graham Greenleaf, "Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience" (2012) 28:1&2 Computer L & Sec R 3-13/121-29; ———"Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners" in Paul Roth, ed*, Privacy law and Policy Review in New Zealand* (Wellington, New Zealand: Butterworths-LexisNexis 2004).

[432] See Colin J. Bennett & Charles D. Raab, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas" (2003) 46 Canadian Public Administration 218; Colin J. Bennett, "Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies" (2011) 2 Journal of Comparative Policy Analysis 13.

political science scholarship.[433] This scholarship has generated various theoretical conclusions relevant to investigating the present context. For example, in her book, *A New World Order*,[434] Slaughter has explored and theorized the role of government networks. For his part, Newman has deployed historical institutionalist scholarship to examine diverse regulatory governance contexts, including privacy and data protection.[435] These scholars have thus developed a range of analytical strategies, conceptual tools, empirical observations, and theoretical propositions that prove pertinent and useful in designing this research.

2.1. Transgovernmental networks

> As several scholars point out, these "organizations" do not fit the model of an organization held by either international lawyers or political scientists — not composed of States and constituted by treaty, they do not enjoy legal personality, and they have neither headquarters nor stationary.[436]

In their review article, *Networking Goes International: An Update,*"[437] Slaughter and David Zaring (Slaughter & Zaring) introduce a historical perspective on the evolution[438] and

---

[433] E.g. Newman extensively analyzed the role of intergovernmental networks—the Working Party in the data privacy context—by drawing on political science theories like historical institutionalism; Bennett utilized the comparative policy analysis approach to conduct comparative studies of various aspects of privacy and data protection.

[434] See Slaughter, "A New World Order", *supra* note 24.

[435] See e.g. Newman & Eberlein, *supra* note 430.

[436] See Slaughter, "Accountability of Government Networks", *supra* note 426 at 355. This article presents an excellent background history on transgovernmental networks. Slaughter traces various evolutionary phases in the emergence of the regulatory state, ranging from epistemic communities (e.g., Basle Committee on Banking Supervision) to a multilayer regulatory system (e.g., the OECD) to the emergence of the EU as a regulatory state to transatlantic governance.

[437] See Slaughter & Zaring, *supra* note 428.

[438] *Ibid*. Slaughter & Zaring reflect back on the scholarly tradition that began with Robert Keohane and Joseph Nye's (1974) work on transgovernmental relations, followed by the emergence of the "international regimes" scholarship (Krasner, 1983). They also identify a second wave of regime theorists that includes Young's (1997) work on NGOs, Haas's (1992) work on epistemic communities, and constructivist work (Picciotto, 2000) on the role of socialization, persuasion and other normative

relevance of transgovernmental networks from a global governance perspective. They explore the following three questions: What are these networks good for? How can we make sure they are good? How do and should they interact with traditional international institutions?[439] These three questions go to the core of the thesis's analytical examination of the role of DPAs (in general) and the Commissioners' Conference (in particular) in international privacy and personal data governance. Also, it is important to reiterate Slaughter's observations about growing IR-IL scholarly interaction, where she claimed that legal scholars have become increasingly aware of the regulatory implications of transgovernmental networks while lacking an "overall conceptual framework for analyzing the resulting interactions as part of international law",[440] and argued for the interdisciplinary synergy.

In another article, Slaughter and Thomas Hale (Slaughter & Hale) [441] described transgovernmental networks as "informal institutions linking regulators, legislators, judges, and other actors across national boundaries to carry out various aspects of global governance."[442] One significant feature of transgovernmental networks is that they are "loosely structured, peer-to-peer ties [among units of different governments] developed through frequent interaction rather than formal negotiation"[443], without supervision from the foreign office or the executive branch. Slaughter & Hale stress that these "networks have arisen in response to the complex governance challenges posed by increasing transnational interdependence".[444] Also, they generally emerge in the "realm of regulatory policy—e.g. commercial and financial regulation, environmental protection—but also extend to judicial and

---

processes. For another excellent review of the transgovernmental networks, see Newman & Bach, "Transgovernmental Networks", *supra* note 430 at 505-528.

[439] See Slaughter & Zaring, *supra* note 428 at 211.

[440] *Ibid* at 215. This point is specifically introduced to illuminate the interdisciplinary relevance of this research project as articulated in Chapter-I.

[441] Slaughter & Hale, *supra* note 428.

[442] *Ibid* at 342.

[443] *Ibid.*

[444] *Ibid* at 343.

even legislative areas of government."[445] The Commissioners' Conference, as a body of national regulators, fits nicely into this category.

Slaughter & Hale categorize the horizontal and vertical dimensions of transgovernmental networks. They also group transgovernmental networks into three broad types: information networks, enforcement networks and harmonization networks. They explain that "the horizontal information networks…bring together regulators, judges, or legislators to exchange information and to collect and distill best practices"[446], whereas enforcement networks aim to co-operate in cross border law enforcement, and harmonization networks seek to achieve convergence over common regulatory practices. All three types of networks have functional overlaps; for example, harmonization networks may serve a regulatory role, like the enforcement networks, while generally having more of a focus on finding common standards than on facilitating cross-jurisdiction enforcement.[447] The Commissioners' Conference is composed of national enforcement authorities but, from a transnational networks perspective, it has primarily manifested the characteristics of a horizontal information network. Slaughter identifies the OECD as the quintessential example of a transgovernmental regulatory network within an established international institution, whose purpose has generally been to convene government officials to address a common problem by making a recommendation or promulgating a model code.[448]

Slaughter raises various concerns about transgovernmental networks. For example, a transgovernmental network created within an international organization may be construed as "relegitimizing the entire organization in the face of rising domestic opposition,"[449] whereas transgovernmental networks established by an executive agreement face the potential problem of "executive collusion to circumvent national legislature". For its part, a spontaneous network "evokes the images of national regulators reaching out across borders to make the world safe

[445] *Ibid* at 342.

[446] *Ibid* at 344.

[447] *Ibid* at 345.

[448] See Slaughter, "Accountability of Government Networks", *supra* note 426 at 355-356.

[449] *Ibid* at 366.

for bureaucracy."[450] Slaughter & Zaring argue that the evolutionary contexts (hence legal foundations) of government networks "can make it harder or easier to integrate government network with existing international organizations or perhaps ultimately to transform them into new ones."[451] None of these specific concerns seems to have been particularly pressing for the Commissioners' Conference. Nonetheless, it is important to be aware of these potential risks, particularly as networks of data protection authorities become new fixtures of privacy and personal data governance.[452]

Another important observation made by Slaughter & Zaring on the implications of transgovernmental networks is that "the existence of networks strengthens incentives for jurisdictions to seek convergence because convergence allows for deeper and broader co-operation."[453] The writers also stress the important role of transgovernmental networks as a "norm-creating phenomenon."[454] Looking specifically at the privacy commissioner networks, it seems that the Working Party created by Data Directive 95/46/EC has been instrumental in generating deeper convergence. However, in other contexts, including the Commissioners' Conference, credible evidence of successful efforts towards such enhanced convergence and norm-development arguably has yet to emerge. That said, two endeavors of the Commissioners' Conference, the Madrid Resolution[455] and the Global Cross Border Enforcement Co-operation Arrangement,[456] have provided indications of the Conference's ambition to take on the normative and convergence assignments. Slaughter & Zaring also underscore the important role of transgovernmental networks as an alternative to the

[450] *Ibid*.

[451] See Slaughter & Zaring, *supra* note 428 at 225.

[452] One might speculate that these risks may arise with respect to GPEN or APPA, as these networks are further assimilated into the broad OECD and APEC organizational infrastructure.

[453] See Slaughter & Zaring, *supra* note 428 at 215.

[454] *Ibid* at 216.

[455] See Madrid Resolution, *supra* note 253.

[456] See Resolution on Global Cross Border Enforcement, *supra* note 290.

"regulatory race."[457] More broadly, they argue that regulatory networks are becoming effective and powerful forms of global governance. These themes of the global governance literature—networks as a potential alternative to the regulatory race, as creators of common standards and as vehicles for addressing globalization—offer interesting avenues for exploring the governance roles of data protection authorities.

One criticism that Slaughter makes of transgovernmental networks is that they are "most likely to spawn fears of runaway technocracy",[458] presenting risks not only of policy collusion but also of the "removal of issues from the domestic political sphere through deliberate technocratic de-politicization."[459] Further, Slaughter and Zaring raise the classic administrative law concern that "the interactions of putative expert regulators risk the development of a regime with little or no public check on administrative actions."[460] However, at the same time, Slaughter suggests ways to address such concerns through heighted transparency or the development of EU-type "information agencies"[461], which lack any coercive powers, but instead play merely advisory roles to policy makers. She describes another common criticism—the claim that these networks constitute mere "talking shops"[462] without any policy-making powers; many are only able to disseminate information, and to bring recommendations and proposals for consideration through the normal domestic or agency rule-making process. She argues that such criticism is short-sighted and claims that in the information age these "talking shops" can serve to generate best practices, codes of conduct, and templates for everything from memoranda of understanding to environmental assessment reviews.[463] Her response to the "talking shops" criticism seems to resonate with the experience of the

[457] See Slaughter & Zaring, *supra* note 428 ("But network regulation avoids the race. Instead of competing with one another, regulators who participate in networks work to create common standards among the diverse jurisdictions with regulators through agreement and copying") at 217.

[458] See Slaughter, "Accountability of Government Networks", *supra* note 426 at 363.

[459] *Ibid* at 363. She referred to the work of Picciotto, "Networks in Economic integration" at 1037.

[460] See Slaughter & Zaring, *supra* note 428 at 220.

[461] See Slaughter, "Accountability of Government Networks", *supra* note 426 at 364.

[462] *Ibid*.

[463] *Ibid.*

Commissioners' Conference, and, to be sure, that platform is actively engaged in proposing fundamental instruments, like the Madrid Resolution, that can provide important insight into the question of what governance models might prove the most viable and constructive.

Slaughter further raises concerns about accountability of transgovernmental networks, with specific reference to external accountability (the accountability of one country to another)[464] and the risk that informal networks in particular might "mask unequal power relationships."[465] Slaughter & Zaring suggest that such concerns might be addressed by invoking standard paradigms of administrative law, like transparency, participation and notice before actions.[466] They also suggest that similar constraints on networks might operate in a global context, a context comprising "traditional state actions, such as treaties… the web of domestic accountability mechanisms that already constrain agencies in their normal activities and that also cover agency participation in networks."[467] Another such constraint can come from other parallel or counterpart networks. The thesis will consider three external factors—statutory foundation, existing international privacy and data protection regimes and the emergence of parallel networks—that have a significant effect on the evolution of DPA alliances, while stressing their statutory foundation as the main constraining factor. Furthermore, Slaughter & Zaring reiterate Slaughter's revised position on the relationship between government networks and traditional international organizations. She identifies three possible relationships: transgovernmental networks can 1) stand alone, 2) complement the efforts of traditional international institutions by facilitating convergence, or promoting co-operation through more formal international agreements by enhancing compliance with existing treaties and other international agreements, and 3) by improving "the quality and depth of co-operation across

[464] *Ibid* at 365. Slaughter conceptualizes both internal and external accountabilities but particularly stresses the role of external accountability in the context of information dissemination by transgovernmental networks. She also lay down various principles to address accountability concerns, like the principle of legitimate difference and positive comity.

[465] See Slaughter & Zaring, *supra* note 428 at 220.

[466] *Ibid* at 221.

[467] *Ibid*.

nations."[468] All of these considerations inform the solutions ultimately recommended by the thesis.

> We recommend moving from the descriptive and explanatory to the normative and prescriptive. In the process, lawyers and political theorists can begin arguing for the creation of networks as viable mechanisms of global governance in some circumstances, particularly in various different relationships to traditional intergovernmental institutions, and *against* [italics in original] them in others where they appear unlikely to be successful, or where the governance costs do not look like they be would be worth the benefits.[469]

Slaughter & Zaring's conclusion defends the relevance of transgovernmental networks in global governance. The writers have made a clear case for considering these venues as new arenas of global governance capable of addressing problems where existing international organizations are unable to cope, and of co-existing with and complementing these organizations under conditions of complex interdependence. In this light, where does the Commissioners' Conference stand in relation to the three existing privacy and data protection regimes, as well as to other evolving parallel networks? The thesis explores this question in the concluding argument of this section.

2.2. Networks of data protection authorities

This section critically analyzes the data protection authorities in the pursuit of two objectives. First, to abstract a conceptual framework which can help to position them in relation to other transgovernmental networks, as elaborated in the preceding discussion. Second, to draw critical observations about the data protection authorities' roles in privacy and personal data governance. Based on these two sets of observations, conclusions about the Commissioners' Conference are developed, with a view to assessing their strengths and limitations in the privacy and personal data governance realm.

---

[468] *Ibid* at 225.

[469] *Ibid* at 226.

> These DPAs have been created by statute and fulfil crucial regulatory functions despite the often unclear, ambiguous and impotent legal provisions that they enforce and interpret… Although DPAs are typically underpowered, their functions go beyond legal enforcement to embrace a variety of promotional and policy-influencing activities and they engage in relationships with those using non-official or extra-legal instruments for the protection of information privacy and the limitation of surveillance.[470]

Raab's observation succinctly conveys the expansive range of roles and functions of data protection authorities.[471] His account enables us to draw a straight line from Slaughter & Zaring's observations about transgovernmental networks to the Commissioners' Conference. Nevertheless, Raab finds Slaughter & Zaring's conceptual framing inadequate in some respects as a description of the DPA alliances. Arguably this is not entirely surprising, as Slaughter & Zaring's account is based on specific transgovernmental networks like the Basle Committee. Moreover, the thesis uses this umbrella descriptive term ("transgovernmental networks") to cover not only the Commissioners' Conference but also other emerging alliances like GPEN. The connecting thread between Slaughter & Zaring's theoretical claims about transgovernmental networks, Raab's focused study of networks of commissioners and the thesis' somewhat broader assessment of international alliances of DPAs is that all of these capture what Raab calls "trends towards global—but therefore multilevel—governance arrangements."[472]

International alliances of data protection authorities (which includes the Commissioners' Conference) fall under the three categories of transgovernmental network identified by Slaughter & Zaring, namely, transgovernmental networks established 1) by an international organization, 2) through states-negotiated executive agreements, and 3) outside of a formal framework altogether by actors seeking to address a common problem. Article 29 of the Working Party created by EU Data Directive 95/46/EC would fall under the first category of

---

[470] See Raab, "Networks for Regulation", *supra* note 26 at 195-96.

[471] *Ibid*. In this article, Raab presents an excellent history of the evolution of the DPAs.

[472] *Ibid.*

international network (here the EU is the relevant umbrella organization); whereas the Commissioners' Conference would fall under the third category, that is, a network developed outside the framework of a formal agreement. Of particular interest would be any new developments towards the emergence of the second category of network—a new transnational regulatory body established by executive agreement, e.g., one created by the EU and the US to implement the recently concluded the Umbrella Agreement, the Privacy Shield arrangement, or any future transnational agreement.

In response to massive transborder data flows as well as the exponential rise in legal enforcement challenges, the data protection authorities have "often expressed alarm in ways that sometimes resemble those of advocacy groups themselves…. [However,] they cannot easily imitate these activists lest they risk being ignored—or perhaps not being renewed in office—by hostile governments or parliaments, or written off by powerful groups which they must often cajole, rather than hector, into more privacy-protective practices."[473] Raab's observation nicely conveys the critical positioning required to thread the needle between being relevant and being redundant. In this light, the DPAs, which are typically constituted as state regulatory agencies, have a delicate balancing job to do in promoting a new binding legal regime. In contrast to Raab's skepticism, scholars like Slaughter seem to have greater faith in the capacities of transgovernmental networks in the context of an evolving world order in which states have become more disaggregated.[474] According to these scholars, such processes of disaggregation have paved the way for the evolution of multilevel governance structures alongside the traditional state-enshrined institutions and international organizations.

Raab has also critically reflected on the entrepreneurship of the DPAs, asserting that "there has been little possibility, so far, of acting together as a global or regional 'rapid reaction force', or of exerting definitive preventative influence in policy-making circles."[475] Despite this criticism, Raab recognizes the DPAs' important role in "establishing the groundwork and

[473] *Ibid* at 196.

[474] See Slaughter, "A New World Order", *supra* note 24 ("It would be a world of disaggregated state institutions interacting with one another alongside unitary states and unitary state organizations") at 35.

[475] *Ibid* at 197.

infrastructure for co-operation and mutual assistance."[476] Moreover, Bennett seems to be in agreement with Raab on this point when he observes that "the role of privacy commissioners has proliferated as well as converged cross-nationally."[477] Raab has also recognized the significance of studying the network of commissioners, stressing that "the activities and perceptions of these officials (and others) about regulatory possibilities and practicalities, about positions to take (or to eschew) on public issues, and about their influence on public policy, commercial practice, and public attitudes and awareness all have a bearing on the nature of regulatory 'races' and their outcome."[478] These observations align with Slaughter's optimism, which ascribes real policy implications to the activities of transgovernmental networks. Raab & Koops have also stressed the importance of permanent "institutionalization" of the network of commissioners, and find "some signs that this network may become more institutionalised and bureaucratised, possibly spawning its own secretariat…. There may possibly be a pay-off in terms of greater influence, or at least voice, in the world's arenas where policies are made that pose threats to privacy."[479]

While Raab & Koops illuminate the general policy impact of the network of commissioners, they fall short on articulating its legal-regulatory roles. Moreover, scholars including Raab and Newman have devoted most of their attention to the institutionalization of the EU-based networks, while failing to consider the prospects for the emergence of parallel networks of privacy regulatory authorities like the GPEN. Raab has approached the analysis of data protection authorities from a multilevel-governance (MLG) theoretical perspective; whereas Newman's theoretical focus has been on the historical institutionalist approach to the study of DPAs in the EU context. Both perspectives are important, but Raab and Koops have warned that the focus on an MLG approach may create "the risk of losing sight of the contribution, and sometimes the pre-eminence, of central states … especially if one were to adopt the

[476] *Ibid.*

[477] See Bennett, "Governance of Privacy", *supra* note 98. He further recognizes multiple contemporary roles for data protection authorities, ranging from ombudsmen to auditors, consultants, educators, policy advisors, negotiators, enforcers, and international ambassadors.

[478] *Ibid* at 198.

[479] See Raab & Koops, *supra* note 99 at 211.

unsustainable position that the Internet, for example, is ungovernable, not least by state activity."[480] Again, this underscores the importance of the thesis' broader approach, which, in contrast to other efforts, insists on including the US-EU case study in order to be able to assess the role of states' interests in privacy and personal data governance.

3. Role of data protection authorities in privacy and personal data governance

What role do data protection authorities play in privacy and personal data governance? Given that the primary focus of the thesis is on international privacy and personal data governance, some brief observations about national privacy and personal data governance are added to paint a comprehensive picture. The following observations and arguments are primarily drawn from the Commissioners' Conference, yet they have potential for generalization to the evolving domain of transgovernmental networks of data protection authorities, like the GPEN. Now that an abstract theoretical framework and the relevant empirical background on the DPAs are in place, we are in a position to draw inferences about their role in privacy and personal data governance as well as to explore the implications of these for the research question and for the alternatives to pursuit of a new, legally binding international instrument that are proposed by the thesis.

What follows is an assessment of the DPAs' governance role in relation to: 1) the existing international regimes, international organizations, privacy enforcement authorities alliances, and national frameworks; 2) the potential for developing a new, legally binding international framework; 3) the institutional evolution of the Commissioners' Conference; and 4) the implications of the foregoing for the thesis's research question and proposed solutions.

3.1. Relationship with international privacy and data protection regimes, international organizations and other alliances of privacy enforcement authorities

The Commissioners' Conference has carefully pursued the relationship-building objective with the adoption of comprehensive strategies. Various adopted resolutions are a testament to these

[480] *Ibid* at 214.

efforts, including the Madrid Resolution[481] and resolutions adopted at other conferences like London,[482] Warsaw,[483] Mauritius,[484] and Amsterdam.[485] The Conference has aggressively sought engagements with national governments and other stakeholders by asking national data protection authorities to play active roles inside their respective states.[486]

A data protection authority, from a national perspective, has multiple leverage points to influence national regulatory policy outcomes all along the spectrum of their assigned roles and responsibilities. For example, in a typical dispute situation, complaint redress or *suo motto* launched investigation, a privacy commissioner or a data protection authority engages in the interpretation of applicable rules, generally drawn from a governing statute and its judicial interpretations. Through this channel, a privacy commissioner can expand or constrain the ambit of the regulatory reach of privacy protection, whether it is settled by resolution of the privacy commissioner or through court litigation. In addition to their statutorily prescribed roles and responsibilities, the data protection authorities also internalize international expertise into national legal and policy frameworks through various channels, like statutory interpretation (governing statute), issue jurisdiction (issues redress), litigation (courts), ministerial advice (amendments and review suggestions), and parliament or legislature reports (annual reports).[487] They also share soft international exposure and information by participating in various policy debates (issues debates), policy representations (consultations and committees) and public awareness campaigns (media reporting and issue discussions).

---

[481] See e.g. Madrid Resolution, *supra* note 253 ("To invite the Data Protection and Privacy Authorities accredited to the International Conference, to disseminate the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, as widely as possible").

[482] See London Declaration, "Communicating Data Protection", *supra* note 198.

[483] See Warsaw Resolution on Conference's Strategic Direction*, supra* note 282.

[484] See Resolution on Global Cross Border Enforcement, *supra* note 290.

[485] See Amsterdam Resolution on Conference's Strategic Direction, *supra* note 291.

[486] See Madrid Resolution, *supra* note 253.

[487] For example, the Office of Privacy Commissioner of Canada (OPC) submits various reports, like its annual or special reports to the Parliament of Canada. See online: OPC <https://www.priv.gc.ca/information/02_05_b_e.asp>.

From an international perspective, the nature of regulatory policy influence depends on the very creation of a data protection authorities' network. In this regard, Slaughter offers useful observations on three key fronts: 1) by identifying three main sources of transgovernmental network formation (international organization, executive agreements, and outside of any formal agreement), 2) by describing the nature of transgovernmental networks along both horizontal and vertical dimensions, and 3) by describing the nature of their assigned roles in terms of information exchange, enforcement co-operation and harmonization. Using Slaughter's categories, it is clear that the data protection authorities' alliances have emerged from all three sources; for example, Article 29's Working Party falls under the first source, the GPEN under the second, and the Commissioners' Conference under the third. Detailed treatment of the Working Party, the expert body created by EU Data Directive 95/46/EC, is beyond the scope of the thesis; whereas the GPEN and other international alliances of DPAs are secondary in importance given their recent emergence and hence limited international footprints to date. The Commissioners' Conference is an example of Slaughter's horizontal network, with predominant characteristics of an information exchange network.

3.2. Development of a legally binding international instrument

On the legally binding instrument, the Commissioners' Conference has adopted a multifaceted approach. The Conference has tended to promote the Madrid Resolution as a foundational instrument upon which future efforts at developing a new, legally binding international framework should build. Raab's assessment seems fair:

> The activities of the international conference group are necessary but insufficient for achieving global regulatory capacity and effectiveness… Madrid Resolution may turn out to have been a plateau rather than a springboard for further institutional development or for more rigorous regulation.[488]

As elaborated in Chapter III, the Commissioners' Conference efforts towards a new, legally binding international framework on privacy and data protection began with the Montreux

[488] See Raab, "Networks for Regulation", *supra* note 26 at 209.

Declaration[489] and its demand for a UN convention. That was followed by the development of a model legally binding instrument, adopted as the Madrid Resolution.[490] It further demanded the organization of an intergovernmental conference[491]; this was followed by an appeal for the adoption of the additional protocol, based on the Madrid Resolution, to Article 17 of *ICCPR*[492]. Recently, the Amsterdam Conference resolution has sought an engagement with the UN Rapporteur on Privacy[493] to work on adopting the additional protocol to Article 17 of *ICCPR*. This seems to represent a clear shift in the Commissioners' Conference's strategy, from dogged pursuit of a new, legally binding international framework for privacy and data protection towards softer approaches. The Commissioners' Conference has also shifted its focus increasingly towards cooperation and collaboration, as illustrated by the Resolution on Global Cross Border Enforcement Agreement[494] adopted in the Mauritius Conference resolution; this stresses heightened collaboration on transnational enforcement measures. This shift in focus also aligns with other parallel initiatives launched at the level of the international privacy and data protection regimes. One example is ongoing EU-APEC collaboration on interoperability between the EU-BCR and CBPR systems.

3.3. Organizational evolution of the Commissioners' Conference

On the institutional evolution of the Commissioners' Conference, the thesis finds clear evidence that the Conference is preparing itself for a long haul. In two resolutions on Strategic Direction adopted at the Warsaw[495] and Amsterdam[496] Conferences, the Commissioners' Conference adopted various strategies to establish itself as a credible stakeholder in privacy

[489] See Montreux Declaration, *supra* note 184.

[490] See Madrid Resolution, *supra* note 253.

[491] See Resolution on Intergovernmental Conference, *supra* note 266.

[492] See Resolution on International Law, *supra* note 232.

[493] See Conference Resolution on UN Privacy Rapporteur, *supra* note 292.

[494] See Resolution on Global Cross Border Enforcement, *supra* note 290.

[495] See Warsaw Resolution on Conference's Strategic Direction, *supra* note 282.

[496] See Amsterdam Resolution on Conference's Strategic Direction, *supra* note 291.

and personal data governance. This supports the thesis' argument that the Commissioners' Conference and other alliances of privacy enforcement authorities represent an emerging fixture of international privacy and personal data governance. These transgovernmental networks of experts are willing to share their experiences and expertise, and are vying to stake claim to the increasingly crowded space of privacy and personal data governance, a space hitherto occupied almost exclusively by traditional national governments and the international privacy and data protection regimes. This attests to Slaughter's proposition that anticipates an increasing role for governmental networks in a globalized world.

Raab has made a strong case for the "institutionalization" of the network of privacy commissioners. Raab's critical assessment of the governance role of the Commissioners' Conference[497] mainly relates to this "institutionalization" aspect.[498] Raab and Koops find the missing organizational structure in the commissioners' network to be one of the main factors that "exemplifies and signifies the general inhibitions on the formation of global regulation and, in this example, the effect of financial and organisational resource limitations, as well as national political and legislative constraints upon the further development of commissioners' roles."[499] They also add that scheduling the annual Commissioners' Conference in a different country every year impinges on its capacity to focus on "issues of the day that affect the working of all in their national contexts, or in agreeing on the very propriety of such concertation."[500]

Raab & Koops argue that "the efficacy of DPAs concerting as watchdogs beyond jurisdictional boundaries is not yet proven and their reputation remains somewhat fragile."[501] At the same

[497] He used the terms network of commissioners or network of world's privacy commissioners quite loosely; Nonetheless, the thesis uses the term the Commissioners' Conference throughout in order to maintain the conceptual consistency.

[498] Raab recognized that the "a number of DPAs and their commissioners have evidently been seized of the necessity to move their vehicle into higher gear, equipping it with the ability to speak and act as an institution with the rules, procedures, boundaries and infrastructure of corporate existence." For details, see Raab, "Networks for Regulation" *supra* note 26 at 203.

[499] See Raab & Koops, *supra* note 99 at 210.

[500] *Ibid* at 211.

[501] See Raab, "Networks for Regulation", *supra* note 26 at 208.

time, they note that the "DPAs have thus emphasized the development of infrastructures for collaboration and have generated a tapestry of interlocking relationships for mutual sharing and regulatory action."[502] Moreover, despite Raab's skepticism, the Commissioners' Conference has recently taken up the matter of institutionalization explicitly, adopting a comprehensive strategy in its Strategic Directions resolution from the recently held Amsterdam Conference.

> DPAs often now see important business interests as well as privacy advocates' groups as their allies in the movement towards global regulation…. these patterns will be described in greater detail, bearing in mind the question of how far this phenomenon constitutes, or promotes, the institutionalization of a multilevel governance infrastructure, perhaps en route to a global regime[503]

Newman provides an interesting insight by building on Keohane and Nye's distinction between transgovernmental co-ordination and transgovernmental coalitions. He observes: "[p]ut bluntly, sub-state actors collaborate cross-nationally when their preferences conflict with their home governments. While transgovernmental coalition building focuses on the politics of rule development, transgovernmental co-ordination centers on the implementation and enforcement of those rules."[504] Newman's observation sheds important light on the renewed emphasis of the Commissioners' Conference on coalition building, as evidenced by the Amsterdam Conference resolution aimed at strengthening connections with "networks involved in cross-border data protection and privacy enforcement", including stronger relationships with "regional forums of DPAs."[505] In addition, the Commissioners' Conference has renewed its focus on seeking "observer arrangements to ensure we have two way effective connections between international organisations and the Conference."[506] Also, the "Resolution on Co-operation with the UN Special Rapporteur on the Right to Privacy" [507] shows the

---

[502] *Ibid*.

[503] *Ibid* at 202.

[504] See Newman, "Watching the Watchers", *supra* note 430 at 184.

[505] See Amsterdam Resolution on Conference's Strategic Direction, *supra* note 291.

[506] *Ibid*.

[507] See Conference Resolution on UN Privacy Rapporteur, *supra* note 292.

Commissioners' Conference's intention to expand the scope of its engagements. The Amsterdam Conference resolutions are strong indications of the intent of the Commissioners' Conference's to engage deeply with other actors in international privacy and personal data governance, whether this be through coordination or coalition building activities.

Moreover, both Slaughter and Raab underscore the utility of inter-network support. Raab emphasizes that "they have recognized the need for mutual support as well as for more institutionalized forms of international collaboration, building upon, but also helping to foster, a variety of emerging networks of relationships that have developed over many years … building on others."[508] Slaughter sees real prospects for the progressive evolution of transgovernmental networks and for their increasingly important place in emerging global governance:

> The challenge for global governance generally is not simply to design multiple institutions to meet multiple challenges, but also to determine how they can best fit together. As long as world government remains infeasible and, for many, undesirable, then the world's capacity to govern itself collectively on the those issues that require collective decision will depend on a patchwork of different kinds of institutions: formal and informal, intergovernmental and transgovernmental, state-based and society-based, durable and flexible. Where transgovernmental networks fit into this picture, or pictures, and how they can best be deployed to strengthen, foreshadow, or replace intergovernmental institutions are rich topics for research and analysis.[509]

3.4. Implications for the regime feasibility question

The following Chapter VI synthesizes the analysis to deliver final observations on the research question; a brief reflection presented here aims to close this chapter's analysis. Besides, the above-developed observations this broad analytical framing of the Commissioners' Conference for the main research question? In light of the conclusions developed to this point, it is fair to

[508] See Raab, "Networks for Regulation", *supra* note 26 at 217.

[509] See Slaughter & Zaring, *supra* note 428 at 225.

make an assertion that the prospect for the emergence of a new, legally binding international framework is minimal. The goal of developing a new, legally binding international privacy regime appears to be overly ambitious, not least in the Conference's own considered view, if its shifting focus in strategy, and increasing attention to developments in other international arenas, are any indication. As we have seen, the Commissioners' Conference has shown a strong interest in, and taken initiatives towards, an enhanced engagement with other governance stakeholders—including existing international privacy and data protection regimes, the United Nations, and other networks of privacy enforcement authorities.

Chapter V. International privacy and data protection regimes and the US-EU confrontations over transborder data flows

Why do we need a new international framework when three international privacy and data protection regimes already exist, and when states can resolve transnational confrontations over transborder data flows through bilateral agreements? The search for answers to this question forms the heart of this thesis. Primary objectives toward this end include expanding our understanding of the *status quo* of existing international privacy and personal data governance, examining ongoing efforts to strengthen that governance, and exploring various potential strategies and solutions.

The following analysis has three elements: 1) to articulate the main theoretical framework that will be used to study this issue (legalization), 2) to examine the empirical dimensions of the issue (the three international privacy and data protection regimes and the EU-US confrontations over transborder data flows) in light of this theoretical framework, and 3) to synthesize the first two elements in order to draw inferences and frame broader theoretical propositions.

Again, it is important to set this chapter in the broader analytical context of the thesis. Thus the purpose of this chapter will be to cover the remaining two analytical components of our attempt to answer the research question,[510] namely the three existing international privacy and data protection regimes and EU-US confrontations over transborder data flows. The earlier analysis in Chapter III surveyed the ongoing governance measures taken by the three international privacy and data protection regimes, and reflected on the agreements between the US and the EU over transborder data flows, with a specific focus on the Safe Harbor agreement. Chapter II supplemented this analysis with a general introduction to the foundations of privacy and personal data governance. The overall analytical objective of Chapters II and III was to provide broad insight into the issue context as well as to illuminate its specific empirical

[510] The previous Chapter IV dealt with the first analytical component, the data protection authorities, with a specific focus on the Commissioners' Conference.

strands. Now, this chapter, by drawing on the relevant theoretical framework, attempts to knit these different strands together to generate a comprehensive analysis that seeks to make contributions on both empirical and theoretical fronts.

The theoretical perspective adopted here derives from IR theory, and draws particularly on the IR literatures on regimes, institutions and legalization. This last literature develops two interesting explanatory strands. The first tries to explicate the rational underpinnings of choices between hard versus soft law. The second deals with the relationship between hard- and soft-law instruments, along a spectrum that ranges from complementary to antagonistic relations. These two accounts are applied to the relationship between the three privacy and data protection regimes, as well as to the pattern of bilateral EU-US confrontations.

The analysis unfolds as follows. First, the theoretical framework of legalization is presented. Second, the relative advantages and disadvantages of hard- and soft-law instruments are explored. Third, the theory is used to explore the two explanatory strands mentioned earlier: 1) the rational underpinnings of hard- vs. soft-law choices and 2) interactions between hard- and soft-law instruments along complementary and antagonistic lines. Fourth, these theoretical conclusions are applied empirically, in order to assess the role in international privacy and personal data governance of the three existing international privacy and data protection regimes and of the transnational confrontations between the EU and the US. Fifth, the implications of the resulting conclusions for the research question, for the governance role of the DPAs, and for the recommended strategies are examined.

1. Theoretical framework—legalization

Chapter IV examined the role of the Commissioners' Conference in international privacy and personal data governance from a theoretical perspective drawn from the global governance literature, with a primary focus on transgovernmental networks. The following discussion examines the role of the existing international privacy and data protection regimes in international privacy and personal data governance, and assesses the implications of EU-US confrontations over transborder data flows for the evolution of a new, legally binding

international framework on privacy and personal data governance, as pursued by the Commissioners' Conference.

The following analysis draws on IR theory, particularly the literatures on regimes, institutions and legalization. The term "regime", according to Steven Krasner (Krasner) means a "set of explicit or implicit principles, norms, rules, and decision making procedures around which actor expectations converge in a given issue-area."[511] Krasner's definition captures, in a broad way, important aspects of law and governance in specific international issue-areas.[512] Nevertheless, it is legalization theory, as articulated by later IR scholars[513] that devotes specific attention to, and presents a compelling analytical framework for, the phenomena of most direct interest to the thesis.[514] More particularly, the notion of legalization, developed by political scientists Kenneth Abbott et al, (in a special issue of the journal *International Organization* entitled "*Legalization in World Politics*"), is selected as the most relevant framework for organizing the analysis. Kenneth Abbott et al define legalization[515] in terms of "a particular set

[511] See Stephen Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables" (1982) 36:2 International Organization 185 [Krasner, "Regime as Intervening Variables"] at 185.

[512] See Stephan Haggard & Beth A. Simmons, "Theories of International Regimes" (1987) 41:3 International Organization 491 at 491-94. The authors argue that regime theory's objective is to fill the theoretical gap between realism and idealism. Among other things, Krasner's definition addresses an important part of the normative dimension of international politics, a part that subsumes institutionalized commitments. Institutionalized normative (legal) commitments were later specifically targeted by the legalization scholarship. Although regime theory delivers important theoretical insights, it is legalization theory that narrows the focus further to explain the phenomena most directly relevant to the thesis.

[513] See Kenneth W. Abbott et al, "The Concept of Legalization" (2000) 54:3 International Organization 401 [Abbott et al, "Concept of Legalization"] at 419.

[514] The legalization literature's main analytical focus is to seek explanations of those aspects of the international politics where states organize their relations through legalized instruments. Legalization is presented as a form of institutionalization with specific characteristics, ranging a spectrum between hard and soft law in three key dimensions: along obligation, precision, and delegation. Our issue-area, international privacy governance, context manifests these features of legalization characteristics across its different institutionalized forms, from the EU framework (hard-law form) to the OECD Privacy Guidelines (soft-law form).

[515] See Abbott et al, "Concept of Legalization", *supra* note 513 at 403 ("Our concept of legalization is a working definition, intended to frame the analytic and empirical articles that follow in this volume as well as future research").

of characteristics that institutions may (or may not) possess. These characteristics are defined along three dimensions: obligation, precision, and delegation."[516] The authors further specify the three dimensions as follows:

> *Obligation* means that states or other actors are bound by a rule or commitment or by a set of rules or commitments. Specifically, it means that they are *legally* bound by a rule or commitment in the sense that their behavior thereunder is subject to scrutiny under the general rules, procedures, and discourse of international law, and often of domestic law as well. *Precision* means that rules unambiguously define the conduct they require, authorize, or proscribe. *Delegation* means that third parties have been granted authority to implement, interpret, and apply the rules; to resolve disputes; and (possibly) to make further rules [italics in original].[517]

Further, along the obligation, precision, and delegation dimensions, they developed a multidimensional continuum, ranging from the "ideal type of 'hard' legalization…. to 'soft' legalization, as complete absence of legislation."[518] In hard legalization, all of the three properties—obligation, precision, and delegation—are maximized, while in soft legalization they exist in various combinations. The specification of these three characteristics is based on core features of rules and procedures, not on effects, and in this draws on H. L. A. Hart's seminal work, *The Concept of Law*,[519] which emphasizes the internalization of the primary and secondary structures of a rule. Another critical insight is the authors' focus on "moving away from a narrow view of law as requiring enforcement by a coercive sovereign"[520]. This focus is mirrored by the thesis's attempt to situate its subject within the broad literature on global governance, as illustrated in Chapter IV's analysis of the data protection authorities.

---

[516] *Ibid* at 401.

[517] *Ibid.*

[518] *Ibid* at 402.

[519] See H. L. A. Hart, *The Concept of Law* (1907-1992) with a postscript, edited by Penelope Bulloch, Joseph Raz, & Leslie Green (Oxford: Oxford University Press, 2012). The authors drew linkages between Hart's abstract concepts of primary and secondary rules and patterns of institutionalization in IR.

[520] See Abbott et al, "Concept of Legalization", *supra* note 513 at 402.

Without delving deeper into the nuances of the legalization concept, this chapter utilizes it to paint a broad picture of the character of international privacy and personal data regimes. From a legalization perspective, the EU regime represents a "hard" regime, as it features the highest threshold along all three legalization dimensions: obligation, precision and delegation. For example, EU Data Directive 95/46/EC has clear stipulations for EU-wide application, requiring all EU members to have a strong national legal framework in order to be in compliance with its requirements. By contrast, both the OECD Privacy Guidelines and APEC Privacy Framework fall under the "soft" form of legalization, as they are generally at the low end of the spectrum of obligation,[521] precision[522] and delegation.[523]

---

[521] *Ibid* at 410-11. (Instruments framed as "recommendations" or "guidelines"—like the OECD Privacy Guidelines on Multinational Enterprises—are normally intended not to create legally binding obligations). Neither the OECD Privacy Guidelines nor the APEC Privacy Framework requires strong commitments from member states. The following is a generalized criterion to assess the nature of obligation:

High
Unconditional obligation: language and other indicia of intent to be legally bound
Political treaty: implicit conditions on obligation
National reservations on specific obligations: contingent obligations and escape clauses
Hortatory obligations
Norms adopted without law-making authority: recommendations and guidelines
Explicit negation of intent to be legally bound
Low

[522] *Ibid* at 405. Again, neither the OECD Privacy Guidelines nor the APEC Privacy Framework have clearly specified the activity covered, nor provided with detailed articulation of fundamental principles. The following range is helpful for understanding their low precision:

High
Determinate rules: only narrow issues of interpretation
Substantial but limited issues of interpretation
Broad areas of discretion
''Standards'': only meaningful with reference to specific situations
Impossible to determine whether conduct complies
Low

[523] *Ibid* at 416. In terms of delegation, both the OECD Privacy Guidelines nor the APEC Privacy Framework have prescribed governing third-party or supranational authority to monitor the implementation and enforcement of the regimes. The following are the indicators of delegation:

a. Dispute resolution
High
Courts: binding third-party decisions; general jurisdiction; direct private access; can interpret and

Apart from the three existing international regimes, another important framework, the EU-US Safe Harbor agreement, is analyzed. Where does the Safe Harbor arrangement stand on the legalization spectrum? Some scholars have described the Safe Harbor agreement as a hybrid type of regulatory arrangement, as suggested in the following:

> The regulatory regime of Safe Harbor therefore consists of several layers: The EU sets the substantive data protection standards, the companies voluntarily commit to them, private or public bodies provide arbitration services, public enforcement is undertaken by a US agency, and the EU Commission still has the last word and can terminate the whole agreement if compliance or public oversight in the US do not work properly. Safe Harbor can therefore be seen as a hybrid arrangement that integrates transnational self-regulation on the one hand, and nation-state based and intergovernmental public regulation on the other hand, into a complex, layered regime.[524]

However, in terms of the legalization parameters set out above, the Safe Harbor agreement

---

supplement rules; domestic courts have jurisdiction
Courts: jurisdiction, access or normative authority limited or consensual
Binding arbitration
Nonbinding arbitration
Conciliation, mediation
Institutionalized bargaining
Pure political bargaining
Low

b. Rule making and implementation
High
Binding regulations; centralized enforcement
Binding regulations with consent or opt-out
Binding internal policies; legitimation of decentralized enforcement
Coordination standards
Draft conventions; monitoring and publicity
Recommendations; confidential monitoring
Normative statements
Forum for negotiations
Low

[524] See Ralf Bendrath, "The Return of the State in Cyberspace: The Hybrid Regulation of Global Data Protection" in Myriam Dunn, Sai Felicia Krishna-Hensel & Victor Mauer, eds, *The Resurgence of the State, Trends and Process in Cyberspace Governance* (Hampshire, England: Ashgate Publication 2007) at 135.

falls at the low end of the obligation spectrum, as the US did not commit to a strong obligation to introduce new legislation, even though it agreed on an oversight framework, albeit with a primary reliance on a self-regulatory approach based on a voluntary registration process and compliance mechanism. Likewise, when it comes to precision, once again over-reliance on voluntary observation and interpretation of the prescribed set of principles pushes it towards the lowest threshold on this dimension. Finally, on the delegation front, US agencies are authorized to supervise compliance, yet the arrangement lacks rigorous enforcement, as US corporations are allowed to opt for self-regulation through third party oversight. Overall, the thesis finds the Safe Harbor agreement to represent a soft-law form of legalization for the purposes of this analysis.

Kenneth Abbott and Duncan Snidal (Abbott & Snidal)[525] argue that "law is an interest-based and a normative enterprise."[526] This claim seems helpful for structuring our analysis. It establishes complementarity between the two leading theoretical perspectives in IR, namely, institutionalism and constructivism, with their central explanatory orientations to interests and norms respectively. There are three ways in which this synthetic theoretical positioning is relevant to this thesis: 1) the nature and scope of the issue, which encompass both normative (e.g., privacy as a human-rights value) and interest dimensions (e.g., data protection in economic and security contexts); 2) the framing of the study in terms of three distinct analytical components (the data protection authorities, three international privacy and data protection regimes and a case study on the US-EU confrontations over transborder data flows)[527] ultimately requires some kind of theoretical synthesis; and 3) the thesis's strategic recommendation to explore the institutionalization of inter-regime co-operation also synthesizes insights from both institutionalism and constructivism. The following analysis expands on this theoretical perspective.

Abbott & Snidal emphasize that "[s]tates and other actors look to law to achieve their ends

[525] See Kenneth Abbott & Duncan Snidal, "Hard and Soft Law in International Governance" (2000) 54:3 International Organization 421 [Abbott & Snidal].

[526] *Ibid* at 425.

[527] *Ibid*. Abbott & Snidal incorporate all three dimensions in various contexts, like the role of NSAs in soft legalization.

whether they are pursuing interests or values."[528] This is the case in the present context too, where the data protection authorities in both the US and EU are pursuing national interests in multiples arenas, including through transnational negotiations. Abbott & Snidal further assert that "[A]ctors utilize both normative and interest-based strategies to create legal arrangements."[529] Again, in the present context, both jurisdictions—the US and the EU—and the data protection authorities have invoked both normative and interest-based strategies. For instance, one of the main strategies adopted by the data protection authorities has been to (normatively) persuade states to engage in international regime development efforts, whereas both the EU and the US have consistently pursued their respective economic interests, manifested throughout the Safe Harbor negotiation process. Moreover, Abbott & Snidal recognize the importance of rules and institutions in terms of "changing material incentives and … modifying understandings, standards of behavior, and identities",[530] utilizing "techniques ranging from litigation and sanctions to persuasion, normative appeals, and shaming."[531] The US-EU confrontations vividly illustrate the utility of multiple strategies adopted by both sides of the Atlantic. For instance, from the inception of the Safe Harbor agreement, the EU side has strategically questioned the agreement's efficacy on multiple occasions, as corroborated by various reports and investigations by EU institutions, like the Working Party and EU Commissions reports and the recent ECJ *Schrems* decision.[532]

These multiple analytical strands and themes represent a synthesized version of institutionalism-constructivism, as envisaged by Abbott & Snidal; examples crop up throughout the thesis's analysis. The thesis does not exclusively subscribe to a specific theoretical approach, but rather develops a rational construct relevant for the analysis of specific contextual dimensions of the issue. In some parts of the empirical account, the analysis may appear to be heavily informed by constructivist perspectives (e.g., in the analysis of the

[528] *Ibid* at 425.

[529] *Ibid.*

[530] *Ibid*.

[531] *Ibid.*

[532] The recent ECJ judgment on the Safe Harbor agreement is testimony to that approach. See, *Schrems* decision, *supra* note 8.

data protection authorities)[533], whereas in others it may appear to conform more closely to institutionalist perspectives (as in case of the US-EU confrontations). This theoretical eclecticism offers the crucial flexibility necessary to organize a comprehensive analysis of the issue. Ultimately, it is the nature of the issue itself that plays the determining role in recommending a synthesized version of both theoretical approaches. The concluding argument in Chapter VI similarly knits these two approaches together—though without explicit allusion to them—to make a strong case for the alternative strategy suggested by the thesis, that is, institutionalization of inter-regime co-operation.

Abbott & Snidal maintain that legalization exerts its effects through "normative standards and processes as well as self-interested calculation, and both interests and values are constraints on the success of law."[534] The potential tensions between these two sets of forces have a parallel in the basic structure of the privacy governance issue. Historically, one of the fundamental drivers of the evolution of the first two major international regimes, the COE 108 and the OECD Privacy Guidelines in early 1980s, was the question of how to ensure the free flow of information across borders while having a minimal impact on privacy rights. The predominant factor underlying harmonization efforts has been the fear of increasing divergence among national laws as a ploy to block the free flow of data; hence, the fear of adverse implications for international trade and transnational commercial activities. The human-rights values dimension was and arguably has always been the secondary consideration throughout the evolution of privacy and personal data governance. The complex tension, and lack of a neat fit, between trade and commerce vs. the right to privacy, or between the free flow of information vs. the security of privacy and personal data, is one of the core centripetal forces dividing the US and the EU.

To conclude, the discussion to this point has addressed two important aspects: the identification, specification and application of a broad conceptual construct of legalization, and the deployment of the theoretical approaches of institutionalism and constructivism that inform

[533] In terms of data protection authorities analysis the previous Chapter IV has presented an explicit articulation of the constructivist theoretical paradigm but this discussion will also reflect back to add more insights.

[534] See Abbott & Snidal, *supra* note 525 at 422.

it. The following section expands on the dynamics of interaction between hard- and soft-law instruments—a discussion that relies heavily on the theoretical arguments of Abbott & Snidal and Shaffer & Pollack—and illustrates these dynamics in the empirical context of our issue.

2. Hard and soft legalization—international privacy and data protection regimes and the Safe Harbor agreement

Gregory C. Shaffer & Mark A. Pollack (Shaffer & Pollack) identify an interesting set of dynamics "between hard- and soft-law instruments as alternatives for international governance". They show "how these instruments can be combined as mutually reinforcing complements", but also argue "that under certain conditions, hard and soft law can and do operate as antagonists [italics in original]."[535] The following analysis develops these insights by specifying and operationalizing in the privacy governance context the explanatory variables that Shaffer & Pollack identify as relevant to the interaction between hard law and soft law. The analysis also considers three different forms of hard-/soft-law interaction, with hard and soft law potentially functioning 1) as alternatives, 2) as complementary, and 3) as antagonistic. These different relationships between hard and soft law are illustrated through the three existing international privacy and data protection regimes and the US-EU Safe Harbor agreement.

Abbott & Snidal examine hard and soft laws as both advantageous and disadvantageous forms of legalization. The authors explore the use of legalization as a form of institution in international governance, examining how and why international actors "choose to order their relations through international law and design treaties and other legal arrangements to solve specific substantive and political problems."[536] Abbott & Snidal's and Shaffer & Pollack's theoretical arguments about hard and soft law are analytically useful in the present context for three main reasons: 1) they set out a broad conceptual framework that can encompass a wide range of existing privacy and data protection frameworks, under the rubric of a hard-to-soft-

[535] See Gregory C. Shaffer & Mark A. Pollack, "Hard Versus Soft Law in International Security" (2011) 52:4 BCL Rev 1147 [Shaffer & Pollack] at 1147. Also available, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1786836>.

[536] See Abbott & Snidal, *supra* note 525 at 421.

law spectrum[537]; 2) they provide a critical reflection on the advantages and disadvantages of hard and soft forms of legalization, and identify the explanatory variables that help (a) to shed light on the interactive relationship among the three international privacy and data protection regimes, and (b) to explain the EU and US positions revealed in the resolution of their transborder data flows confrontations, mainly in the form of the Safe Harbor agreement; and, finally, 3) they support the thesis' central argument about the institutionalization of inter-regime co-operation, further developed in Chapter VI.

Hard law, according to Abbott & Snidal, is comprised of "legally binding obligations that are precise … and that delegate authority for interpreting and implementing the law,"[538] and is adopted by actors to "reduce transactions costs, strengthen the credibility of their commitments, expand their available political strategies, and resolve problems of incomplete contracting". However, it comes with a cost, as it "restricts actors' behavior and even their sovereignty."[539] Again these arguments are important for understanding the implications of hard law, particularly as it has been envisioned by the Commissioners' Conference as a solution to the problem of international privacy and data protection. As for soft law, Abbott & Snidal simply describe it as a "broad class of deviations from hard law",[540] and argue that soft law has its own utility, and in some respects offers better solutions than hard law, because it is easier to achieve. To underscore the advantages of soft law as an efficacious tool under certain circumstances, Abbott & Snidal list "a number of variables—including transaction costs, uncertainty, implications for national sovereignty, divergence of preferences, and power differentials—that influence which forms of soft law, which combinations of obligation, precision and delegation, are likely to be selected in specific circumstances."[541] The thesis uses some of these explanatory variables to explicate the US-EU positions on privacy and personal data governance as revealed in their ongoing confrontations.

---

[537] This aspect is dealt with earlier in this chapter.

[538] See Abbott & Snidal, *supra* note 525 at 421.

[539] *Ibid* at 422.

[540] *Ibid* at 422.

[541] *Ibid* at 423.

Vis-à-vis the relative advantages and disadvantages of hard vs. soft law, it is clear that each has its own value and can serve different underlying objectives. However, one should also note that they are not binary instruments, as they can overlap and complement each other. In a same issue-area they can co-exist and even thrive in parallel. Abbott & Snidal use "contract" and "covenant theory" to further elaborate the functions of hard and soft law. "States enter into 'contracts' to further interests; they enter into 'covenants' to manifest normative commitments",[542] argue Abbott & Snidal. Before moving to a detailed analysis, it is important to understand the importance of these points in light of the overall analytical framework of the thesis, which is based on three analytical components: the data protection authorities, the three international privacy and data protection regimes and the US-EU confrontations. To recall Abbott & Snidal's arguments, they stress hard law's advantages as including the reduction of transactions costs, strengthening of the credibility of actors' commitments, expansion of actors' available political strategies, and resolution of problems of incomplete contracting, whereas its disadvantages come down to restrictions on actors' behavior and sovereignty. The following discussion will further elaborate these theoretical points, with the main focus being on the "sovereignty cost" variable.

Abbott & Snidal recognize legalization as one of the "principal methods by which states can increase the credibility of their commitments."[543] By applying contracting theory, they assert that "credible commitments are crucial when one party to an agreement must carry out its side of the bargain before other parties are required to perform [theirs]... [c]redible commitments are essential whenever some parties to a strategic interaction demand 'assurance' from others". One example might be when "a government … would suffer domestic political costs if the other party reneged; it would therefore demand credible assurances."[544] In the case of the US-EU negotiations preceding the conclusion of the Safe Harbor agreement, the EU aggressively sought from the US every assurance about the protection of the data privacy rights of EU citizens. Towards that end, the EU rejected the adequacy of the US self-regulatory approach

[542] *Ibid* at 424.

[543] *Ibid* at 422.

[544] *Ibid* at 426.

and pushed the US to incorporate provisions for oversight by an appropriate US government agency. Despite accepting oversight by agencies such as the FTC, the US maintained the self-regulatory approach as non-negotiable and inserted its "nuanced" version of oversight in the Safe Harbor arrangement.

Despite the deeply held skepticism of various concerned stakeholders in the EU, the EU Commission supported the Safe Harbor agreement as an adequate framework for the transfer of EU citizens' personal data. But two recent events—Snowden's revelations about the NSA surveillance program and the ECJ's *Schrems* decision on the US Safe Harbor agreement—not only brought US credibility into question once again but also raised questions about the EU Commission's authority, given its earlier approval of the Safe Harbor agreement. Even though the Safe Harbor agreement is clearly a soft form of legalization, it is also primarily a credibility-establishing arrangement between the EU and US. The *Schrems* case, which has rendered the Safe Harbor agreement invalid, illustrates how US credibility has been affected. It is in order to obtain assurances about the credibility of US commitments to the privacy of transborder data flows that the EU has consistently pushed the US towards a strong domestic regime for privacy and data protection. If the Safe Harbor agreement had been a harder legalized instrument and had been respected, the US surveillance capacity would presumably have been limited, as such would have been required by the strong commitment. By contrast, in the context of the actual Safe Harbor agreement, to use Abbott & Snidal's terms, the "costs of reneging" were minimal for the US. From a hard law perspective, the US actions would have attracted a heavy reputational cost, given the prior existence of bilaterally sanctioned rules and standards; they would also be likely to lead to fixed consequences for the violations, since the violation of enforcement measures would normally involve countermeasures from the other party.[545] Moreover, hard legal commitments generally give rise to domestic legal transplantation through legislative measures or through the litigation route;[546] hence, they raise the prospect of alterations to the established national legal framework, which in turn has

[545] *Ibid* at 427.

[546] *Ibid*. (Abbott & Snidal referred to Ellen L. Lutz and Kathryn Sikkink's observations about "how international rules condemning torture and other atrocities have been characterized as customary international law and applied by U.S. courts") at 428.

important implications for domestic constituencies and increases the audience costs to the government of violations. These theoretical insights resonate very well in the EU-US Safe Harbor agreement context, and help to explain the stances of each side.

Another useful observation about hard legal commitments is that they can "mobilize legally oriented interest and advocacy groups"[547] and can help to legitimize their participation and establish their credibility in domestic decision-making. In the context of the Safe Harbor agreement, on the US side, NGOs like EPIC and CDT have consistently maintained pressure for a comprehensive legal framework for the protection of US citizens' privacy rights; however, they have been unable to translate this pressure into legislative terms. More interestingly, at the EU level, where the character of the legal commitments established by the COE 108 and Data Directive 95/46/EC is rigorous and exhaustive, legalization has incentivized interested non-state parties to challenge the Safe Harbor agreement through court litigation, as illustrated strikingly by the recent Court of Justice of the European Union (ECJ) judgment on *Maximillian Schrems v. Data Protection Commissioner*.[548] Besides legitimacy and reputational costs, another normative implication of legalization is that it imposes a specific form of discourse "requiring justification and persuasion in terms of applicable rules and pertinent facts, and emphasizing factors such as text, precedents, analogies, and practice."[549]

Abbott & Snidal formulate several hypotheses about independent variables likely to lead states to adopt hard legal commitments. Of particular interest:

> First, states should use hard legal commitments as assurance devices when the benefits of co-operation are great but the potential for opportunism and its costs are high.
>
> Second, states should use hard legalization to increase the credibility of

[547] *Ibid* at 428.

[548] See ECJ *Schrems* decision, *supra* note 8.

[549] See Abbott & Snidal, *supra* note 525 (Abbott & Snidal highlight the underlying constructivist logic with their assertion that "[l]egal discourse largely disqualifies arguments based solely on interests and preferences") at 429.

> commitments when noncompliance is difficult to detect…[550]

> Third, [as reformulated from the demandeurs' perspective:] … [d]emandeurs should seek hard legalization (1) when the likelihood of opportunism and its costs are high, and noncompliance is difficult to detect.[551]

To reflect briefly on these hypotheses in the context of the US-EU confrontations: on the EU (the demandeurs') side, the emphasis on the credibility of commitments was apparent as the EU consistently sought strong assurances and adequate compliance from the US. But for the US this was not the case, even though the benefits of co-operation were potentially very high so long as the resulting agreement preserved weak U.S. privacy protection practices.[552] What other features of the Safe Harbor agreement context might explain US behavior? A brief look at other dimensions of legalization, like the reduction of transactions costs, suggest that hard law can serve states' interests and can deliver positive benefits unavailable to those who pursue soft-law instruments. The existence of hard law reduces the costs of subsequent interactions involving the elaboration and enforcement of rules that have already been agreed upon. "Compared to alternatives like frequent renegotiation, persuasion, or coercion, it materially reduces the costs of enforcement,"[553] argue Abbott & Snidal. One might expect the U.S. to desire the benefits of reduced transaction costs and thus to pursue hard law; but in fact it took the counter position, insisting on a soft law arrangement in the form of the Safe Harbor agreement. Why was this the case? The following section cites the "sovereignty cost" explanatory variable to answer this question.

The contracting costs for hard legalization are high, as they involve negotiating costs including the drafting of legal instruments by legal professionals and most critically getting the arrangement approved through legislative authorization. Costs related to its violation are also

---

[550] *Ibid* at 429.

[551] *Ibid* at 431.

[552] *Ibid* (Abbott & Snidal assert that "[o]f course, other things being equal, states that resist agreement or desire greater flexibility should resist hard legalization") at 432.

[553] *Ibid* at 431.

very high. However, once a hard legalization is in place its compliance and enforcement costs are significantly reduced.[554] Let us again reflect on the US-EU negotiations on the Safe Harbor agreement. Representatives from the EU Commission and the Office of the US Trade Representative engaged in a heated, prolonged negotiation. On the US side, going through the normal channel of congressional approval was not an option. Thus, the EU and the US negotiators came up with an innovative implementation and supervision scheme in the form of the Safe Harbor agreement, one that bypassed the need for authorization by US congress and avoided any introduction of legislative changes.

"States, jealous of their sovereign autonomy, are reluctant to limit it through legalized commitments", claim Abbott & Snidal. Similarly, Shaffer & Pollack emphasize that as hard law restricts state behavior and infringes on sovereignty, "states may bargain fiercely and at length over hard-law agreements."[555] Is preservation of sovereign autonomy the major factor behind the U.S. desire to limit the obligation and delegation dimensions of the Safe Harbor agreement? By contrast, soft legalization mitigates sovereign autonomy costs either through incorporating escape clauses, putting in place imprecise commitments or imposing legislative oversight over delegation. "These institutional devices protect state sovereignty and reduce the costs and risks of agreement while providing some of the advantages of legalization",[556] observe Abbott & Snidal. This point is important for the development of the thesis' argument in Chapter VI. The two scholars show how international nuclear and trade regimes[557] have utilized various institutional tools of soft legalization to deliver optimal outcomes without imposing strong regimes, which would have come with heavy costs in various guises. Furthermore, Abbott & Snidal underscore the trade-off dynamics between hard and soft legalization, as both forms come with relative costs. Moreover, Abbott & Snidal identify a

[554] *Ibid* at 434.

[555] See Shaffer & Pollack, *supra* note 535 at 1163.

[556] See Abbott & Snidal, *supra* note 525 at 435.

[557] *Ibid* at 435-36. They describe how two leading international nuclear regimes, the Nuclear Non-Proliferation Treaty and International Atomic Energy Agency, as well as the General Agreement on Tariffs and Trade and subsequent World Trade Organization (WTO), utilized such legalization forms and strategies.

series of independent variables that determine the nature of the costs attached to hard- and soft-legalization choices. These independent variables are: sovereignty costs, uncertainty, divergent national preferences, differences in time horizons and discount rates, and power differentials among major actors.[558] Of this list, sovereignty costs are most strongly manifest in the EU-US confrontations, and significantly condition the outcomes along all three dimensions of legalization—obligation, precision, and delegation.

3. Sovereignty cost—implications on the EU-US confrontations

The thesis has adapted Abbott & Snidal's arguments about sovereignty costs to shed light on the US-EU confrontations over transborder data flow in the context of the Safe Harbor agreement. Sovereignty cost helps to explain the US stance in its confrontations with the EU. Generally, where sovereignty cost is high, states are less willing to commit to hard legalization. On the other hand, when sovereignty cost is low states are more inclined to agree on hard legalization.

For Abbott & Snidal sovereignty costs are comprised of three categories which influence states' choices on legalization: potential for inferior outcomes, loss of authority and diminution of sovereignty, Though the following analysis does deploy these categories, on their own they are too broad-brush to deliver adequate insight into this issue. Instead, Krasner's more differentiated conceptualization of sovereignty is better suited to assess the sovereignty dimensions of US-EU confrontations leading up to the Safe Harbor agreement. Abbott & Snidal summarized Krasner's notion of sovereignty in the following words:

> Krasner offers four meanings or categories of sovereignty: *domestic* sovereignty (the organization of authority and control within the state), *interdependence* sovereignty (the ability to control flows across borders), international *legal* sovereignty (establishing the status of a political entity in the international system), and *Westphalian* sovereignty (preventing external actors from influencing or determining domestic authority structures). Krasner 1999. These categories overlap

[558] *Ibid* at 436.

> and do not covary in any necessary pattern. [Italics in original][559]

One dimension of Krasner's conceptualization of sovereignty that is significant in this context is interdependence sovereignty.[560] Interdependence sovereignty seems to capture some important aspects of our empirical case. For example, US-EU confrontations over transborder data flows demonstrate an intrinsic complexity and seem to be premised on the difficulty of unilateral efforts to control the flow of information across borders. On the other hand, *Westphalian* sovereignty[561] may be implicated in the EU's assertion of transnational authority via Data Directive 95/46/EC, which imposed a strong third-country adequacy assessment requirement as a pre-condition for the transfer of data to a third country. The EU has aggressively pursued adequacy assessment of third countries, partially as a way of promoting the expansion of EU standards of privacy and data protection. That pursuit by implication interferes with a third country's domestic privacy and data protection framework. Hence, from the US perspective it amounts to the transplantation of the EU approach into its domestic legal regulatory framework. This implicates the concept of *Westphalian* sovereignty, as it amounts to a serious interference in the United States' domestic authority. This extraterritorial reach of EU Data Directive 95/46/EC caused intense debate in the US and heated trans-Atlantic confrontations between the EU and the US from the very inception of the Data Directive in the late 1990s. Moreover, there are also implications for domestic sovereignty,[562] which are instructive in the present context:

> The loss of interdependence sovereignty, which is purely a matter of control, would

[559] *Ibid* at 436-37. For an extended version of Krasner's conceptualization of sovereignty, see Stephen D. Krasner, "Abiding Sovereignty" (2001) 22:3 International Political Science Review 229 [Krasner, "Abiding Sovereignty"]. Krasner presents a useful review of sovereignty from the perspective of both rationalist (realist and neoliberal institutionalist) and constructivist theories of international relations. He surmised that "[S]overeignty' resilience is, if nothing else, a reflection of its tolerance for alternatives") at 229.

[560] *Ibid* (According to Krasner, "[I]nterdependence sovereignty refers to the ability of states to control movement across their borders") at 231.

[561] *Ibid* ("Westphalian or Vettelian sovereignty refers to the exclusion of external sources of authority both *de jure* and *de facto*") at 232.

[562] *Ibid* ("Domestic sovereignty refers to authority structures within states and the ability of these structures to effectively regulate behavior") at 231.

> also imply some loss of domestic sovereignty, at least domestic sovereignty understood as control, since if a state cannot regulate movements across its borders, such as the flow of illegal drugs, its is not likely to be able to control activities within its borders, such as the use of these drugs.[563]

These overlapping formulations of sovereignty cost help define the nature of the outcomes of US-EU confrontations in the context of transborder data flows. The thesis argues that the EU attempt and temptation to impose the EU Data Directive 95/46/EC regime on the US necessarily implicates the sovereignty cost variable; hence the strong US stance against any such efforts. It doesn't mean that the US is totally unwilling to negotiate and resolve the issue of transborder data flows with the EU. As long as negotiation and resolution of the issue allows the U.S. to avoid a high sovereignty cost, it would be willing to engage. But the important consideration is the degree of sovereignty diminution. For the US, the sovereignty cost threshold is very high, should the EU model risk being transplanted into its domestic framework. As a consequence, the Safe Harbor agreement exhibits its present design, with both the US and EU having compromised on soft legalization or a hybrid regime.

This empirical account of the US-EU negotiations, and of their outcome in the form of the Safe Harbor agreement, yields two contestable propositions: the first speculates on the US position; the second on that of the EU. On the US side, future engagement with the EU on transborder data flows appears to have reached a deadlocked situation where the US is willing to pursue transnational negotiations so long as this does not require commitment to a strong domestic legal regulatory regime, which by implication renders very unlikely the emergence of any hard legalized agreement between the EU and US. By contrast, a consistent demand for, and persistent push towards, hard legalization through bi/multi-lateral negotiations seems to be the approach favored by the EU for the time being. Notably, the EU has been able to force other countries to adopt higher thresholds on privacy and data protection in their domestic legal frameworks.

Overall, the interdependence, *Westphalian* and domestic dimensions of sovereignty underpin

[563] *Ibid* at 232.

the US-EU confrontations and help us understand and explain the character of the states' behavior. The following section further specifies the sovereignty cost variable in term of the nature of the issue-area, focusing in particular on its connections to security and trade. On the security dimension, both the US and the EU have recently concluded the Umbrella Agreement. With respect to commercial data flow, a new regime is on the horizon, in the form of the recently negotiated Privacy Shield arrangement. Despite these latest developments, the main focus of the thesis is on the Safe Harbor agreement.

Abbott & Snidal advance the following open-ended hypothesis about the impact of sovereignty-cost considerations, allowing for a wide range of state responses that will depend on the nature of the issue-area:

> Viewing constraints on national autonomy and sovereignty as costs that vary across issues, we hypothesize that states will prefer different forms of legalization in different issue-areas.[564]

Two issues that have received increasing attention in connection with privacy and data protection, national security and political economy, receive particular attention here. As national security involves extreme sovereignty costs, hard legalization is very unlikely to emerge, because states want to preserve maximum autonomy. Political economy, by contrast, involves a wide range of issues and corresponding legalization forms. Generally, trade-related issues involve low sovereign costs but greater benefits; hence, the incidence of legalized agreements is very high. According to Abbott & Snidal, in trade-related issues the "sovereignty costs are significant but are frequently outweighed by the perceived benefits of legalized agreements."[565] Again, to reflect on the US-EU confrontations, the Safe Harbor agreement is deeply embedded in trans-Atlantic trade dynamics, whereas the PNR and the recently concluded "Umbrella Agreement" more strongly implicate the security dimension, at least with respect to state surveillance, if not necessarily traditional national security with its connotations of war and military conflict. Thus, the trade-security juxtaposition complicates the US-EU

[564] See Abbott & Snidal, *supra* note 525 at 440.

[565] *Ibid* at 441.

transnational agreement environment. Where trade considerations dominate, the Safe Harbor agreement embodies soft legalization. In the security context, although the PNR transfer agreement sets out a simple policy framework, the EU-US Umbrella Agreement involves hard legislative measures, as revealed in adoption of the *US Judicial Redress Act*.

Now, with respect to the Safe Harbor agreement, the sovereignty cost for the US was significant, but the benefits outweighed those costs. To specify the sovereignty cost along the hard-to-soft-legalization spectrum, the sovereignty cost imposed by the Safe Harbor agreement falls on the lower end of the scale, as the framework does not commit to strong legal obligations and demands minimal delegation to independent tribunals or supranational dispute resolution bodies. As the US was under tremendous pressure from local constituencies, mainly the multinational corporations, to address the adverse consequences of Data Directive 95/46/EC, the overall assessment of benefits pushed the US to negotiate with the EU. This meant that given US interests, agreement was possible, but only at a low threshold (soft legalization). To sum up: the nature of the issue-area implicated in negotiations over transborder data flows implied a severe sovereignty cost for the US, were it to adopt the hard legalization demanded by the EU; this therefore explains the substance and structure of the Safe Harbor agreement.

Despite the extensive advantages of soft law, it can come with considerable costs. Does the Safe Harbor agreement provide the US with substantial leeway to escape its commitments? The ongoing Snowden revelations speak to the fact that the US had no binding legal obligation under the Safe Harbor agreement that prevented, or could prevent, it from engaging in massive surveillance.

Abbott & Snidal raise concerns that "[s]oft law compromises make it harder to determine whether a state is living up to its commitments and therefore create opportunities to shirk."[566] The continued secret operation of the US NSA surveillance program appears to attest to such opportunities insofar as enforcement of the Safe Harbor agreement is concerned. "[Such compromises] also weaken the ability of governments to commit themselves to policies by

[566] *Ibid* at 446.

invoking firm international commitments and therefore make it easier for domestic groups, including the very same branches of government, to undo the agreement,"[567] emphasize Abbott & Snidal.

The following discussion expands the scope of the analysis to interactions between hard- and soft-law forms. Shaffer & Pollack, in their article, *Hard Versus Soft Law In International Security*,[568] present an insightful analysis of the relationship between hard and soft forms of law. They apply their conclusions to the study of two empirical contexts, namely "the legality of the threat or use of nuclear weapons, and the legality of the use of force in humanitarian intervention under the 'responsibility to protect' doctrine."[569] Their analysis is important in the present context for four main reasons: 1) it presents a general framework for understanding the relationship between hard and soft law as either alternative, complementary or antagonistic options; 2) it develops a specific theoretical framework for studying antagonistic relationships between hard and soft law, formulating specific hypotheses that are operationally useful for our analytical purposes; 3) the general theoretical model helps advance the thesis's objectives of exploring the interrelationship between the three international regimes, shedding additional light on the data protection authorities' initiatives, and critically examining the US-EU Safe Harbor agreement; and 4) it provides support for the thesis' argument about institutionalization of inter-regime co-operation, further developed in Chapter VI.

4. Inter-regime interaction—complementary and antagonistic

The previous sections primarily treated hard and soft law as alternative options, examining the advantages versus the disadvantages of hard and soft legalization. This section draws on Shaffer & Pollack's arguments about the two other forms of interaction between hard and soft law that they identify: complementary and antagonistic relationships. Shaffer & Pollack's description of the evolution of international law—from initial concerns with the codification

[567] *Ibid* at 446.

[568] See Shaffer & Pollack, *supra* note 535.

[569] *Ibid* at 1147.

and progressive development of international law to the more recent focus on new law-making—helps to explain why and how international legal scholarship has shifted its focus away from traditional customary and treaty-based law towards the hard- and soft-law characteristics of new international instruments, as well as "the relative advantages and disadvantages of these characteristics in different contexts, and how these instruments can be used progressively as complements."[570] The complementary relationship between hard and soft law works along two dimensions: "soft law may develop over time and harden into hard law" and "hard law may be elaborated, extended, and progressively developed through soft law."[571] The following analysis dwells on these two dimensions of the progressive evolution of law, asking: how are they manifested in the context of international privacy and data protection governance?

As we have seen, the US-EU Safe Harbor agreement is a soft-law agreement that resulted from acrimonious negotiations between the EU and the US. The point now is to explore whether it can develop over time into hard law or progressively move towards that end. Such an exploration would be directly relevant to our interest in examining the feasibility of developing a new, legally binding international framework. Two recent developments[572] need further consideration before exploring the prospects for progressive hardening of the agreement.

First, the EU and the US have recently concluded the Umbrella Agreement, which aims to put in place a high-level data protection framework for EU-US law enforcement co-operation. The Agreement covers all personal data (for example names, addresses, criminal records) exchanged between the EU and the U.S. for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism.[573] The key feature is that the EU citizens "will have the same judicial redress rights as US citizens in case of privacy

[570] *Ibid* at 1156.

[571] *Ibid* at 1156-57 (Defines this phenomenon as a form of "progressive development of law").

[572] These developments involve the recently concluded Umbrella Agreement, the recent ECJ decision in the *Schrems* case, and the implications of ongoing EU data protection reforms.

[573] See European Commission, Press Release Database, "Questions and Answers on the EU-US Data Protection 'Umbrella agreement'" (8 September 2015), online: European Commission <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>.

breaches"[574], which will extend "the core of the judicial redress provisions of the US Privacy Act of 1974 to EU citizens"[575] and will formally come into existence once the US passes the *US Judicial Redress Act*. This major development—along with the PNR transfer arrangements between the US and the EU—indicates some progress towards legalization, yet in a targeted and limited fashion.

The second development relates to commercial trans-Atlantic data transfer, where the EU Commission recently released the text of the newly negotiated Privacy Shield arrangement. Again, it is important to underscore that the Privacy Shield is only the very latest arrangement and that it will further evolve during its implementation phase. In any case, the thesis retains its analytical focus on the Safe Harbor agreement. All the same, the emergence of the EU-US Umbrella Agreement and the EU-US Privacy Shield provides interesting glimpses into the ongoing evolution of international privacy and personal data governance.

Despite its rapid evolution, the trans-Atlantic privacy and data protection legalization pattern has a couple of reliably stable features: the EU is unwilling to compromise its citizens' data protection rights, whereas on the other hand the US is willing to compromise in only a very limited fashion its lax position on privacy protection. As we have seen, for the US a commitment to hard legalization imposes a high sovereignty cost, particularly in the commercial data flow context. The proposition that soft law may develop over time and harden into hard law might lead one to detect a shift towards hard law in the recently concluded Umbrella Agreement or the Privacy Shield program. But to insist that such departures—if this is indeed what they are—represent a major change in the US approach that will bring it more in line with the EU model would be a speculative leap, particularly in light of the thesis's central argument. Where the US is concerned, the main argument has been that the sovereignty cost for hard legalization imposes a very high threshold, one quite unlikely to be breached. Hence, the thesis anticipates a prolonged deadlock between the US and the EU over transborder data flows. This argument has additional implications for the research question, implications elaborated in the concluding chapter.

---

[574] *Ibid*.

[575] *Ibid*.

Now, the second form of complementarity identified by Shaffer & Pollack is the possibility that hard law can be elaborated, extended and progressively developed through soft law. A credible argument can be made that even though Safe Harbor was by its nature a soft law, the agreement actually did much to enhance the credibility of the EU's existing hard-law regime. Various countries around the world have internalized the EU model into national legal regulatory frameworks. These soft law channels have proven critical for expanding the scope and reach of the EU's data protection framework, which elsewhere may take forms that are not necessarily as hard as those implemented in the EU member countries themselves.[576]

The contention that the EU framework is expanding its global reach can be defended, insofar as that framework can probably be fairly characterized as the most effective and influential model currently in play. However, one should not take this as confirmation that international privacy and personal data governance has been fundamentally Europeanized. In conclusion, the evolutionary patterns in international privacy and personal data governance show a constructive synergy and strategic voluntary alignment that have established the increasing role of the EU regime in international privacy and personal data governance. Whether it is hard law being supplemented by soft laws or soft law being progressively translated into hard law, the EU regime matters along both dimensions.

Both propositions—that soft law may develop over time and harden into hard law, and that hard law may be elaborated, extended, and progressively developed through soft law; or in other words, non-binding soft law can lead the way to binding hard law, whereas soft-law instruments can subsequently elaborate existing hard law[577]—hold promise for the future evolution of international privacy and data protection frameworks. The thesis topic involves both hard- (EU) and soft- (the OECD Privacy Guidelines and APEC Privacy Framework) law forms of international regimes on privacy and personal data governance. The EU regime is already hard law, and that puts it in the center of the evolution of international privacy and personal data governance. But how do these different forms of interaction between hard and

[576] One such area of potential is the ongoing international co-operation between the EU-BCR and the APEC-CBPR systems on interoperability, with the possible prospect of making inroads into national laws. See, EU-APEC Interoperability, *supra* note 39.

[577] See Shaffer & Pollack, *supra* note 535 at 1165.

soft law manifest themselves in relations between the OECD and APEC privacy regimes?

The OECD Privacy Guidelines and APEC Privacy Framework are also important sites of soft-law evolution, with good chances of supplementing the evolution of hard law, as well. Are ongoing measures at the OECD and APEC levels actually themselves moving towards hard law? This seems unlikely, for such a move would run counter to their very existence; these regimes were meant to be soft by design, in the first instance. Nevertheless, ongoing developments, particularly relating to enhanced transborder collaboration among the DPAs of member states in information sharing and enforcement measures, seem to indicate positive developments for international privacy governance without imposing any legal obligation or extra delegation. These efforts are supplementary, and not contrary, to the existing frameworks. For example, the OECD recommendation on cross-border co-operation and collaboration (2007) among the data protection authorities, and APEC's measures on enforcement collaboration and interoperability, are steps that have expanded the scope of soft-law measures. Shaffer & Pollack argue that under certain situations, when existing hard law encounters new and unforeseen circumstances, soft law may provide a low-cost and flexible way to elaborate and fill in the gaps".[578] These ongoing regime modification efforts, at both the OECD and APEC levels, seem to represent just this sort of gap-filling strategy.

As for antagonistic relationships between hard and soft law, Shaffer & Pollack argue that antagonism can arise from the conflicting distributive implications of law and legal change, especially for powerful states. Shaffer & Pollack contend that "[u]nder conditions of high distributive conflict and high regime complexity, we are likely to see hard and soft law often interacting as antagonists."[579] Distributive conflict encompasses the "distribution of absolute gains from co-operation among two or more states rather than relative gains as conceived in the Prisoner's Dilemma game."[580] Thus, under conditions of high distributive conflict and regime complexity, "states and other actors may deliberately use soft-law instruments to undermine hard-law rules to which they object or, vice-versa, to create an antagonistic relationship

[578] *Ibid* at 1165-66.

[579] *Ibid* at 1157.

[580] *Ibid* at 1167-68.

between these legal instruments."[581] These arguments shed significant light on US and EU interactions over transborder data flows. Analogously, the concepts of regime complexity and regulatory fragmentation seem to capture patterns in the international privacy and personal data governance context, where a wide array of national and international governance instruments, regimes and legal-regulatory frameworks exists. (In ways resembling the realm of cyber space, which Joseph Nye has characterized in terms of regime complexity.)[582] Given the conceptual complexity involved, Shaffer & Pollack's formulation of explanatory hypotheses is helpful. The following two testable hypotheses in particular seem to nicely capture the pattern of EU-US confrontations:

> Hypothesis 1. Where distributive conflict is low between powerful states, they are likely to deploy hard and soft law to work as complements in an evolutionary manner.[583]
>
> Hypothesis 2. Where distributive conflict among powerful states is high, we are more likely to see them deploy hard and soft law in opposition to each other, often by working through different international regimes and fora. These overlapping hard- and soft-law regimes and fora, in turn, may come into conflict. When they do, the soft-law regimes and fora can lose some of their technocratic, flexible, and deliberative features, and the hard-law regimes and fora can become less clear and determinate in their requirements. Where distributive conflict is ongoing, international legal instruments will not simply converge into a new synthesis, but may remain in conflict for a prolonged period.[584]

With respect to the first hypothesis, Shaffer & Pollack survey the literature in international economic law, and argue that where both the US and EU agree on a policy or rule they can

---

[581] *Ibid* at 1172-73.

[582] See Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities", Global Commission on Internet Governance Paper Series No. 1, online: CIGI <https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities>.

[583] See Shaffer & Pollack, *supra* note 535 at 1175.

[584] *Ibid* at 1176.

promote it globally, and such agreement is considered an important factor for successful international regulation.[585] Thus, to apply the hypothesis to the US-EU confrontations, the distributive conflict dimension suggests a higher threshold for the US. Consequently, the US agreed only on a very narrow and targeted approach, adopting the Safe Harbor agreement in order to protect its national interests.

Of particular interest is the second hypothesis, which speculates about scenarios of high distributive conflict among powerful states and their implications for the antagonistic deployment of hard and soft law. Now, it could be defensible to surmise that the US has activated various international privacy and data protection regimes and fora in order to neutralize the expansion of the EU regime. Three critical instances require attention in this regard. First, in the wake of EU Data Directive 95/46/EC and its implications for US trade and commercial interests, the US was able to maintain the self-regulatory design embedded in the Safe Harbor agreement regardless of EU pressure for a comprehensive legal commitment. Second, the US has promoted other international measures, such as the OECD Revised Privacy Guidelines, that explicitly stress the effectiveness of self-regulatory and technological measures. Third, the US is a major promoter of various measures at APEC, like the CBPR System,[586] which directly compete with EU Data Directive 95/46/EC's binding corporate rules (BCR). However, the EU has taken notice of the development at APEC and launched initiatives towards interoperability between the EU-BCR and the APEC-CBPR system. The thesis argues that the US strategically engages with international fora through soft-law measures deployed in an antagonistic fashion to counter EU advances and leadership in international privacy and personal data governance. That does not, however, mean that the EU is losing the contest. Rather, it has aggressively pursued and promoted the EU data regime though various Directives that impose stringent requirements. Various scholars have argued for the expanding role of the EU in global standard setting in general, including privacy and

[585] *Ibid* (They quoted Daniel Drezner's argument that an agreement between the United States and the EU is both a "necessary and sufficient condition for successful international regulation") at 1175.

[586] For the CBPR system, see the section on APEC measures in Chapter III above. The U.S. has been actively engaged in promoting the CBPR system. The US Federal Trade Commission acts as a backstop regulator, whereas the US-based privacy seal provider, TRUSTe Inc., is the first accredited accountability agent.

personal data governance.[587]

The second hypothesis predicts that "[w]here distributive conflict is ongoing, international legal instruments will not simply converge into a new synthesis, but may remain in conflict for a prolonged period"[588]. This would seem to tally with the thesis's central argument, which anticipates a serious, ongoing deadlock between the US and EU. Such a conclusion would have implications not only for the research question but also for the overall future of the evolution of international privacy and personal data governance, including the potential development of a new, legally binding international framework, as proposed by the Commissioners' Conference.

5. Role of international privacy and data protection regimes and trans-national agreements (EU-US Safe Harbor agreement) in privacy and personal data governance

Our chosen theoretical framework has been used to explore the role of three existing international privacy and data protection regimes and to assess the implications of ongoing EU-US confrontations over transborder data flows.

On international privacy and data protection regimes, the first conclusion confirms that regimes matter. The three international regimes on privacy and data protection play crucial roles in governance, both from a bottom-up and a top-down perspective. The EU's COE 108 and EU Data Directive 95/46/EC, the OECD Privacy Guidelines, and the APEC Privacy Framework were all created by member states to address the issue of privacy and data protection, with a specific emphasis on national legal regulatory harmonization. The actual degree of national harmonization varies in terms of the degree of obligation and delegation embedded in each regime: for EU member countries there is limited scope for derogation from Data Directive 95/46/EC's regime; whereas the OECD Privacy Guidelines and APEC Privacy Framework

[587] E.g. Shaffer & Pollack explicitly recognize the EU's strength: "The EU, however, has played an increasingly entrepreneurial role in global governance, from standard-setting to climate change to financial regulation, attributable in large part to the increased institutionalization and harmonization of European regulation at the EU level." Shaffer & Pollack, *supra* note 535 at 1175-76.

[588] *Ibid* at 1176.

provide member countries with significant leverage, owing to their flexibility on enforcement and implementation measures. Both, the OECD Privacy Guidelines and the EU framework has been source of considerable international recognition beyond the member states the OECD Privacy Guidelines due to its flexibility, and the EU, by contrast, on account of the stringency of its third-country adequacy requirements. The EU framework's hard legalization formulation has resulted in transnational confrontations, most significantly those with the US over transborder data flows. On the other hand, all three regimes are further evolving to address emerging challenges: just as the OECD modified the OECD Privacy Guidelines of 1981 with the Revised Privacy Guidelines of 2013, the EU has launched the modernization of COE 108, with Data Directive 95/46/EC soon to be replaced by a new framework, while APEC has also adopted various new measures like the CBPR system. Moreover, when regarded through theoretical lenses, all three privacy and data protection regimes have been a major source of international norms development in privacy and data protection. For example, the APEC Privacy Framework draws significantly on the OECD Privacy Guidelines, and EU Data Directive 95/46/EC has influenced various countries' national data protection frameworks worldwide.

Regarding inter-regime relations, all three international privacy and data protection regimes have stressed the importance of international co-operation and collaboration. However, recent developments have supplemented these affirmations with more concrete measures. The need for collaboration is made increasingly pressing by the global penetration and expansion of transborder data flows activities, which have raised challenges for information exchange, enforcement co-operation, and resolution implementation measures. Therefore, various efforts are underway to address these emerging challenges, with a renewed emphasis on inter-regime co-operation and collaboration. The EU-APEC joint project on interoperability between the EU-BCR and the APEC-CBPR further illustrates that drive.[589]

[589] E.g. the Article 29 Working Party established by the EU Data Directive 95/46/EC and the APEC Data Privacy Sub-Group are actively engaged in streamlining the EU-BCR with the APEC-CBPR system. For further details, see Chapter III, section on the APEC initiatives.

Moreover, there does not seem to be evidence that indicates any serious antagonism among the three international privacy and data protection regimes. Rather, the evidence suggests continued complementary interactivity going all the way back to the parallel evolution of the OECD Privacy Guidelines and COE 108 in the 1980s. The three privacy and data protection regimes are well established in their own right and seem to focus more on international co-operation and collaboration than on competing with one another to establish a single regime as the superior alternative. Furthermore, the thesis has explored interesting developments at the OECD and APEC that appear to have expanded the scope of the existing privacy and data protection regimes through constructive measures, particularly with respect to co-operation over transborder enforcement and implementation measures. Although soft-law in character, these various measures have demonstrated the abiding interest in further adaptation and modification of national legal regulatory approaches. These soft forms of legalization, according to Shaffer & Pollack, can promote the evolution of hard law either through their eventual transition to hard law or by adding new dimensions to existing hard law through elaboration. The convergence over a privacy principles-based approach exemplifies this pattern. Either way, soft law moves toward, or contributes to, hard law. This yields an interesting hypothesis to be tested: whether the strategic shift at the OECD and APEC revealed in these ongoing measures will amount to the hardening of soft law as those regimes further evolve remains to be seen.

Another focus in our exploration of the existing privacy and data protection regimes has been their role in the potential development of a new international regime. So far, the Madrid Resolution is the closest thing we have to a formal expression of this proposition to develop a new regime. However, its vision for achieving that proposition might warrant some skepticism, given our reflections to this point. Generally, any new regime based on existing divergent regimes will be constructed on the basis of a common denominator. That common denominator will generally involve a minimal threshold in order to bring the diverse regimes together. It is true that under certain circumstances, like Shaffer & Pollack's antagonistic scenario, one regime may trump or replace the other regime(s). This might be an alternative to creating a new regime based on a lowest common denominator. Yet this is not the approach pursued by

the Commissioners' Conference's Madrid Resolution[590], which is based on the existing privacy and data protection regimes, including the OECD Privacy Guidelines and APEC Privacy Framework. The hard-law design and ambitions of the Madrid Resolution therefore demand further scrutiny. The thesis has suggested that the Resolution represented an effort of the Commissioners' Conference to consolidate its international position as a strong voice and crucial stakeholder in international privacy and personal data governance. But this pragmatic consideration aside, one might hypothesize that in substantive terms, the Commissioners' Conference has essentially been promoting, and attempting to upload, the European model in international privacy and data protection governance. Such a hypothesis might be put to the test by conducting an extensive examination of the evidence regarding the evolution of the Madrid Resolution. In contrast to the Resolution, a lowest-common-denominator-based instrument drawn on the three existing international privacy and data protection regimes would no doubt yield a predominantly soft-law design, if its aim were in fact to create alignment and harmony among the divergent regimes.

With respect to the US-EU confrontations, the account has focused on sovereignty cost as an explanatory variable that has played a central role in determining the outcomes of the confrontations leading up to the conclusion of the Safe Harbor agreement. Sovereignty cost is anticipated to be high in hard law, low in soft legalization, with the choice depending on the nature of the issue area. In international trade and economic activities, sovereignty cost is generally assumed to be low, and the likelihood of hard legalization correspondingly high; whereas, conversely, in the national security context, the sovereignty cost is high, as is the likelihood of soft legalization. However, this binary set of outcomes is not the only possibility: in certain circumstances, even if the sovereignty cost is high, the anticipated benefits may outweigh that cost and can lead to a hard-law agreement. The thesis has further refined the sovereignty-cost variable by incorporating the dimensions of interdependence and *Westphalian* sovereignty. On this basis, in examining the Safe Harbor agreement, the thesis has argued that for the US the sovereignty cost in transborder data flows is very high, so high even that the commercial and trade benefits failed to outweigh it. The thesis illustrated considerations of

[590] See Madrid Resolution, *supra* note 253.

interdependence and Westphalian sovereignty by pointing to the extraterritorial reach of EU law, and the possibility of its transposition into the US national legal framework, as concrete evidence of the (high) anticipated sovereignty cost of a hard-law outcome.

Based on this assessment of the implications of sovereignty cost, the thesis anticipates a prolonged deadlock between the US and the EU over transborder data flows issues. That deadlock has three implications. First, the US will continue to hold its present strategy of addressing any further challenges through targeted bilateral agreements, as evident in the case of the recently concluded Umbrella Agreement. Second, drawing on Shaffer & Pollack's antagonistic hypothesis, the thesis argues that the US will continue to explore and to deploy other international arenas to neutralize the EU push for the development of a strong global privacy and data protection standard. One extended implication of this argument is that the US might be unwilling to support the Commissioners' Conference, or might even activate other platforms to counter the Conference's efforts to advocate strongly for the development of a new, legally binding international regime. Third, the EU is likely to keep up its strong pressure on other states and to promote the EU model wherever possible. Outside of the deadlock with the US, the EU has enjoyed some success in applying pressure on other countries like Canada and Australia. There is no indication that the EU will retreat from that path in the near future. It would instead be reasonable to anticipate that the recent *Schrems* decision of the ECJ, and the ongoing drive to overhaul its data protection framework, will further expand the scope of the EU's transnational confrontations.

To conclude: what are the implications of these conclusions for the research question? The analysis of the three international privacy and data protection regimes has found no evidence of real inter-regime antagonism or any appetite for trying to advance one regime over the others. The three privacy and data protection regimes formulate the bedrock of international privacy and personal data governance today, and they have launched various measures and joint projects towards enhanced international co-operation and collaboration. Given all this, the likely prospects for the emergence of a new, legally binding international privacy and data protection regime are very low; the three existing international privacy and data protection regimes are here to stay. Similarly, the ongoing US-EU confrontations over transborder data flows reveal strong evidence of a prolonged deadlock between the world's two leading

economies, both with very high stakes in international privacy and personal data governance. In the shadow of such a deadlock scenario, the development of a new global regime, which would ultimately have to be based on a US-EU consensus, is unlikely to happen.[591]

Thus, based on the conclusions reached so far, it seems reasonable to assert that the development of a new, legally binding international framework for privacy and data protection, as pursued by the Commissioners' Conference, is not feasible, at least under the prevailing circumstances. Alternatively, the thesis argues for the institutionalization of inter-regime co-operation, a proposal further developed in the following chapter.

[591] E.g. Raab stresses that "the USA …– has no comprehensive Federal data protection legislation, … [yet its] stance on privacy regulation is all-important to any global achievement." For additional details see Raab, "Networks for Regulation", *supra* note 26 at 208.

Chapter VI. Conclusions, research outcomes and suggested alternatives

1. Conclusions

This chapter has three objectives: 1) to provide a detailed overview of the thesis' overall analysis; 2) to knit the thesis' research outcomes together within the analytical orientation of the research question; and 3) to explore potential solutions through the recommended alternative approach, which argues for reorienting efforts towards the institutionalization of inter-regime co-operation.

The thesis' research began with a refection on the current *status quo* of international privacy and personal data governance. In an evolving internet- and information- communications-technology-based global society, the issue of privacy and data protection has emerged one of the formidable challenges faced by everyone from privacy policy makers to online service providers. Interest in this issue-area further expanded with the evolving post-9/11 surveillance society, as illustrated by Snowden's ongoing revelations about the US-NSA surveillance program. Thus, in a fast-paced, evolving global information age witnessing the rise of the surveillance state, the problems of privacy and data protection have made it harder for the existing national and international frameworks to address emerging challenges. Consequently, any new privacy and personal data governance instruments essentially have to be global in breadth and scope. Given the limitations of existing territorially-bound national measures and the prevailing divergence among the existing international privacy and data protection regimes, demands for the development of a new, legally binding international framework have acquired considerable traction, with the Commissioners' Conference leading the march. The shifting terrain of the issue-context, with the wide diffusion of global personal information and its important implications for the economy, technology and security, has resulted in the emergence of multiple stakeholders, such as privacy advocates, civil society organizations, alliances of international data protection authorities, and so on. Thus, the inherent complexity of the issue, the involvement of multiple stakeholders, the divergence among national and international privacy and data protection regimes, and the increase in trans-national confrontations have further complicated the task of policymakers, legislators and administrators in developing effective tools to address the emerging challenges.

In order to understand the evolution of the global information society and the surveillance state with their substantial implications for privacy and data protection, the thesis conceived a research design grounded in an overarching research question. The research question was then addressed through a governing analytical framework that required consideration of three main analytical components, *viz*., the data protection authorities, the existing international privacy and data protection regimes, and evolving transnational solutions resulting from US-EU confrontations over transborder data flows. Chapter I introduced the overall analytical design of the thesis, along with a brief summary of its main outcomes. Further, a case was made for adopting an interdisciplinary research orientation that would draw on recent scholarship investigating the relationship between international relations and international law. Central to the analysis was the main research question:

> *Given existing international conditions, is the development of a new, legally binding international framework on privacy and data protection feasible?*

Chapter II illuminates the foundation of privacy law. It was organized around two main dimensions. First, it provided a conceptual framework for international privacy and data protection, based primarily on the definition enshrined in the OECD Privacy Guidelines. This definition was supplemented by existing work on the conceptualization of informational privacy. Second, it delivered a broad-brush reflection on the foundations of the existing national and international privacy and data protection frameworks. The overall objective of this chapter was to provide readers with additional information on the issue-context from a more comprehensive angle

Chapter III dealt with the empirical context of the issue and sought to achieve two objectives: 1) to illuminate the nature of the emerging challenges, by placing the issue of privacy and personal data protection in the broader context of the rise of an internet- and ICT-based global information society and of the surveillance state; and 2) to examine the nature and scope of recent strategies for dealing with these challenges, as these have emerged in three international venues, namely, the Commissioners' Conference, the three existing international privacy and data protection regimes, and the transnational bargains hammered out in the context of EU-US confrontations over transborder data flows. In the first instance, a strong case for the need for actions to address the emerging challenges is presented. In the second, stock is taken of

ongoing governance efforts at each of the three international venues. The latter assessment comprises the bulk of the chapter's analysis.

First, there is the Commissioners' Conference, with its demand for, and ensuing initiatives towards, developing a new, legally binding international framework. By contrast, we also have the three existing international privacy and data protection regimes, engaged in consistent updating and modification of their respective frameworks. Somewhere in between these alternatives are the emerging transnational arrangements adopted in the course of ongoing confrontations between the US and the EU over transborder data flows. These three venues collectively represent a generic set of potential governance strategies: (1) seeking the development of a new international regime, (2) further adaptation and modification of existing international privacy and data protection regimes, and (3) allowing the states to resolve transnational privacy and data protection issues themselves through bilateral arrangements. This dynamic pattern represents the current *status quo* in the evolving realm of international privacy and personal data governance.

With respect to the Commissioners' Conference, the thesis surveyed the resolutions adopted at its annual conferences (2005-15) in order to ground observations about: (1) its relationship with international organizations, existing international privacy and data protection regimes, and other privacy stakeholders, including other alliances of privacy enforcement authorities; (2) a shift over time in its focus, from developing a legally binding international framework to a soft-legalization approach that emphasizes enforcement co-operation and collaboration; and (3) strategies the Conference had adopted to establish its international credibility and presence through specific resolutions for its institutionalization. With respect to the three international privacy and data protection regimes, the chapter primarily assessed ongoing governance measures at the OECD, EU and APEC. The specific focus was on existing forms of inter-regime co-operation and ongoing collaboration especially on enforcement and information exchange. With respect to the EU-US confrontations, the focus was on the Safe Harbor agreement, though substantial attention was also given to EU Data Directive 95/46/EU's approach to third country data transfers.

Chapter IV developed a theoretical framework for assessing the data protection authorities, focusing specifically on the Commissioners' Conference. The framework was informed by the

literature on transgovernmental networks in global governance. Slaughter's work in particular was used to link theoretical arguments about transgovernmental networks to the data protection authorities. These arguments were then used to assess the strengths and limitations of the data protection authorities' role in international privacy and personal data governance, along both national and international dimensions. Various venues and opportunities that data protection authorities can use to influence privacy and personal data governance were identified, with the goal of underscoring their growing governance role. In the chapter's conclusion, the thesis found strong prospects for an enhanced role of the data protection authorities in the future evolution of privacy and personal data governance. However, with regard to their specific aim of developing a legally binding international framework, the thesis raised serious doubts.

Chapter V drew extensively on legalization theory in international relations scholarship in order to critically examine the role of the three existing international privacy and data protection regimes and to assess the implications of EU-US confrontations for the overall evolution of international privacy and personal data governance. The concept of legalization was operationalized along a hard-to-soft-law spectrum, and the relationship between the three regimes was assessed in terms of both its potentially complementary and antagonistic dimensions. The thesis found no evidence of deep inter-regime antagonism, and stressed rather the deep-rooted complementarity to be found in their pattern, both historical and ongoing, of collaboration. With respect to the EU-US confrontations, the main explanatory variable—sovereignty cost—was operationalized in order to specify and explain the nature of the relevant (US and EU) states' national interests. This chapter concluded with some initial observations about the research question and set out the theoretical support for the alternative arguments proposed by the thesis.

Finally, this chapter concludes the thesis by synthesizing the main outcomes. Its aim is mainly to knit the theoretical analyses of Chapters IV and V together with the empirical content of Chapters II and III, and to examine the resulting whole in relation to the research question initially posed.

2. Research outcomes

Based on the detailed analysis of the three analytical components, the answer to our research question is that the emergence of a new, legally binding international framework on privacy and data protection is very unlikely. Now the question becomes: if a new, legally binding international privacy regime is unlikely to emerge, then what should be done? Does the *status quo* hold the better prospects, or should some other alternative be explored? The thesis certainly recognizes the significance of the ongoing measures currently being developed in international privacy governance particularly at the three main international venues. The Commissioners' Conference is not only consolidating itself as a powerful stakeholder, but also laying the groundwork for an expanded role for other non-state actors in international privacy and personal data governance. Similarly, all of the international privacy and data protection regimes have launched various measures to address some of the emerging challenges. Finally, various states have devised innovative tools to address challenges related to transborder data flows. The thesis' argument is that the scattered character of these ongoing efforts, in a context marked by deep-rooted inter-regime divergence and prevailing differences among the national frameworks, demands further concerted initiatives to explore new strategies. One such initiative has been launched by the Commissioners' Conference, with its demand that a new, legally binding international framework be developed—an initiative that the thesis ultimately suggests is not feasible.

Therefore, the thesis argues for the reorientation of governance efforts, from the attempt to build a legally binding international regime towards the institutionalization of inter-regime cooperation. This suggestion has a precedent in existing inter-regime co-operation[592], but it would further expand such collaboration [593] and would strategically align with the

[592] Inter-regime co-operation has been one of the central features of the three existing international privacy and data protection regimes. The OECD Privacy Guidelines and COE 108 evolved simultaneously through close co-operation, and, as we have seen, the APEC Privacy Framework adopted the OECD Privacy Guidelines' privacy-principles-based approach. For an extended discussion of inter-regime co-operation, see Chapter III's discussion of the international regimes' ongoing initiatives.

[593] For example, the ongoing collaboration between the EU and APEC on interoperability of the EU-BCR and the APEC-CBPR system. See Chapter III, above for additional details.

Commissioners' Conference's institutionalization efforts.[594] The following discussion further develops this argument. Before that, however, a detailed synthesis of the main conclusions about the three analytical components is presented.

With respect to the data protection authorities, Raab asks the relevant questions about the ongoing activities of the Commissioners' Conference:

> Does the spate of procedural, organizational and public relations initiatives constitute merely the actions of an aspiring global regulatory force getting all dressed up with rules and procedures, establishing an identity and a "mission", but with nowhere to go? Or are they the necessary groundwork preparations for more effective global regulation?[595]

The thesis argues that there is little basis for cynically interpreting the emerging alliances of data protection authorities, or the Commissioners' Conference in particular, as ephemeral or as outsized ambition "all dressed up with nowhere to go". The expanding scope of the international alliances of data protection authorities, like the Global Privacy Enforcement Network, constitutes strong evidence of their relevance. Nearly across the board, the international privacy and data protection regimes have not only given the PEA alliances substantive consideration but have also explicitly approved and promoted them as important actors in international privacy and personal data governance. The establishment of GPEN at the behest of the OECD is testament to that fact. The thesis finds that prospects for further international collaboration among data protection authorities are strongly supported by various recent initiatives, like the Commissioners' Conference's resolution on Global Enforcement Cooperation.[596]

The thesis' analysis of the Commissioners' Conference points to a key role for the data protection authorities in both the national and international arenas of privacy and personal data

---

[594] See Chapter III's discussion of the Commissioners' Conference's ongoing efforts towards institutionalization.

[595] See Raab, "Networks for Regulation", *supra* note 26 at 209.

[596] See Resolution on Global Cross Border Enforcement, *supra* note 290.

governance. Although a data protection authority is a national regulatory body created under a governing statutory framework with prescribed roles and responsibilities, the statutory mandate generally leaves wide latitude for the data protection authorities' engagement in national and international privacy and personal data governance. In the national arena, apart from their statutorily prescribed legal enforcement rights, these authorities are generally vested with wide discretionary powers significant enough to exert influence on the national privacy and data protection legal-regulatory landscape. Similarly, in the international arena, they participate in activities related to international privacy and personal data governance in order to share information, expertise and experience; they have also set up a broad platform for public dialogue that has played an important in engaging multiple stakeholders and drawing attention to critical issues requiring legislative attention.

Based on the extensive analysis of the Commissioners' Conference resolutions, the thesis develops three main observations. First, there has been a noticeable shift in its focus away from a legally binding international framework and towards a soft-legalization option, such as seeking the UN's engagement through adoption of an additional protocol to Article 17 of the *ICCPR.*[597] Second, there is recent evidence of an enhanced focus on further engagement with the international privacy and data protection regimes, international organizations (e.g. with the UN through its Privacy Rapporteur), and other stakeholders, including other PEA alliances. This renewed focus has responded to, taken account of and mirrored expanded collaboration efforts in those arenas.[598] Third, the Commissioners' Conference has continued to work towards its own institutionalization.[599] However, this does not mean that the Commissioners' Conference has totally abandoned the proposition of developing a legally binding regime; the evidence suggests merely a reorientation in its focus, at least for the time being. On the other

[597] This is one of the main conclusions reached by the Commissioners' Conference, as discussed in details in the previous Chapter III.

[598] For example, two resolutions on the Conference's Strategic Direction (Warsaw and Amsterdam) have made this objective as their main focus. For extra details, see Chapter III, above, section on the Commissioners' Conference initiatives.

[599] For example, now the Commissioners' Conference has a dedicated website (icdppp.org) and also established the secretariat service provided by the New Zealand's privacy commissioner's office.

hand, the thesis does argue that whether a new, legally binding international regime on privacy and data protection is feasible largely depends on how it would synchronize with the three existing international privacy regimes, as well as how it would accommodate states' national interests. Such a synchronization effort was partially rationalized in the Madrid Resolution[600], but that resolution fell short on accommodating national interests—at least those of the US—from the thesis' perspective. Nonetheless, the thesis recognizes the significant role of the data protection authorities in any future evolution of international privacy and personal data governance, whether that relates to pragmatic policy-making or other regime-development challenges.

As far as the international privacy and data protection regimes and the US-EU confrontations are concerned, Chapter V considers the central role of the existing international privacy and data protection regimes in privacy and personal data governance. By specifying these regimes along a hard-vs.-soft-legalization spectrum, the thesis applies the theoretical insights of Abbott & Snidal and Shaffer & Pollack to the present context. The main findings highlight the complementary inter-relationship among the privacy regimes. All of the three international privacy and data protection regimes have not only stressed the importance of international co-operation and collaboration but have also taken various measures and joint projects to further enhance such inter-regime co-operation. The thesis explores the role of both the OECD and APEC privacy regimes' efforts in supplementing the hardening of international norms, as evident in the OECD Revised Privacy Guidelines and APEC's interoperability initiatives. Irrespective of the Commissioners' Conference's efforts towards developing a legally binding regime, the thesis found no evidence of realistic prospects for their replacement. Rather, the thesis argues that the existing international privacy and data protection regimes not only play the central role in influencing national and international privacy and data protection frameworks, but also offer the site of first response to member states to address emerging challenges. The international privacy and data protection regimes are one of the most viable and constructive sources for developing international privacy norms, as their evolution is backed by the member states through a legitimate institutional process. This bottom-up

[600] This rationalization of the synchronization effort refers to the fact that the Madrid Resolution draws on the existing international regimes, as discussed in detail below.

approach has unique advantages in addressing a constantly evolving issue-area with sufficient flexibility and efficiency, in contrast to the imposition of a top-down, hard-legalized regime.

In terms of the ongoing US-EU confrontations, the main finding of the thesis is to anticipate a prolonged deadlock between the US and EU over issues related to transborder data flows. Based on a detailed analysis of the Safe Harbor agreement, the thesis found that for the US the sovereignty cost of committing to hard law is very high, even though having a strong regime in place promises to deliver substantial benefits in terms of credibility, cost and efficiency. On the other hand, the EU has long been recognized as the leading force on the international scene in privacy and data protection, having succeeded on many occasions in imposing its strong regime on other countries. The thesis argued that antagonistic undercurrents might drive US posturing on this issue, as it has pursued and activated other venues to counter EU pressures to transpose the strong European model to the international and national arenas. Thus, the ongoing US-EU deadlock has serious implications for the overall evolution of international privacy and personal data governance. Without a consensus between the US and EU, the prospects for the emergence of a strong global regime on privacy and personal data governance are minimal.

Thus the thesis' analysis culminates in the conclusion that, under current circumstances, where three leading international privacy and data protection regimes are continually adapting and modifying their respective structures in order to respond to emerging challenges, and where deep divergence between the US and the EU approaches over transborder data flows has emerged, the likelihood of the development of a legally binding international framework, as pursued by the Commissioners' Conference, is minimal. Therefore the thesis argues for an alternative approach.

3. Suggested alternatives—-institutionalization of inter-regime co-operation

> Some authors have speculated on the future of privacy protection in a globalizing world, and assessed the economic and political factors constraining or promoting either a regulatory "race to the bottom" or a "race to the top".[601]

[601] See Raab, "Networks for Regulation", *supra* note 26 at 197.

In light of the above-quotation, it is reasonable to ask: what is the future of privacy and personal data governance? Will it be a race to the top or bottom, or will the *status quo* prevail? This thesis does not subscribe to either of these scenarios, but instead makes a cautiously optimistic argument for an alternative approach. Thus, based on the extensive analysis of the three main international privacy governance arenas that have substantial stakes in international privacy and personal data governance, the thesis argues for exploring the institutionalization of inter-regime co-operation. This argument charts a middle course, based on finding that a new international regime on privacy and personal data protection is unlikely to emerge as well as rejecting the notion that *status quo* offers the best future or at least a sustainable path for privacy and data protection. Does the institutionalization of inter-regime co-operation reformulate the Commissioners' Conference approach? If not, then in what way does it offers a better solution? The following discussion elaborates these questions. Conceiving a governance framework of global reach is an ambitious endeavour, and such a criticism might well be made of the thesis' argument for the institutionalization of inter-regime co-operation. To put matters bluntly, any such endeavor would require far more research and resources than those utilized by the thesis. Therefore, that objective falls beyond the scope of this research project. Nonetheless, the following observations are offered in order to defend the basic rationale behind this tentative proposal that emerges from the thesis' findings.

First, institutionalization has unique advantages. Raab, though speaking specifically about the Commissioners' Conference and not global privacy governance as a whole, interprets the ongoing efforts of the Commissioners' Conference as a move towards some sort of institutionalization. Supporting empirical evidence in this regard can be found in the adopted resolutions of the Commissioners' Conference (e.g., the Amsterdam Conference resolution, Strategic Directions).[602] Any form of institutionalization creates a certain degree of permanency, with some kind of administrative setup ranging from securing office space to setting up a document repository. This is more on the administrative and technical side. From that perspective, institutionalization of inter-regime co-operation can create a degree of permanency and establish administrative and other resources.

[602] See Amsterdam Resolution on Conference's Strategic Direction, *supra* note 291.

Second, institutionalization is generally based on a common ideological and normative foundation and designed to serve explicitly identified and agreed-upon common interests. When it comes to privacy and personal data governance, the thesis has presented a strong evidence of a convergence on underlying values, privacy principles and general objectives, as illuminated in various international and national privacy and personal data governance instruments. For example, all three international privacy and data protection regimes have converged on a general privacy-principle-based approach, with minor variations. The historical interactivity and mutual borrowings among the three privacy regimes illustrates this common core. Common goals, objectives and convergence on principles offer fertile ground for constructing a substantive instrument.

But why should the recommended institutionalization draw on inter-regime co-operation? Five reasons are relevant here. First, there is the fact that the existing international privacy and data protection regimes have historically drawn on each other, and have taken their own constructive measures to address emerging challenges as those have arisen. For example, the OECD adopted the Revised Privacy Guidelines in 2013, APEC launched the Pathfinder project aiming to enhance cross border enforcement co-operation, and the EU continues to explore a broad range of new measures and rules. Second, all three international privacy and data protection regimes have expanded existing inter-regime co-operation with additional measures, like the joint EU-APEC initiative to enhance interoperability of the EU-BCR and APEC-CBPR systems. Third, the three privacy and data protection regimes have evolved within the umbrella framework of larger international organizations. This has important implications for credibility and legitimacy: they already have the backing of the organizations' member states. Fourth, the evolution of new norms through the three privacy and data protection regimes is more likely to produce minimal frictions among states, as those norms would evolve through a bottom-up process whereby they would be agreed upon and vetted by those states before they even became the subject of debate or part of a regime. Finally, from the perspective of state interests, the existing privacy and data protection regimes are devised to serve member countries individually as well as collectively. States have created these regimes as their first line of defense to defuse international tensions. Therefore, before states would engage in any new regime-formation efforts, they are bound to access the current reservoir and to assess the

implications of their existing commitments. For these reasons, the three existing privacy and data protection regimes offer more fertile ground for developing a new framework.

The thesis research has generated a reservoir of findings which can used to speculate on the possible forum and substance of the proposed institutionalization. With regard to the forum, Slaughter's arguments may again be useful. According to her thesis about the contested/disaggregated state, in conditions of global governance with complex interdependence, the likelihood of the co-existence of multiple structures and arenas of governance is high. Such multi-level governance structures are pervasive features of globalization. These new governance forums can impinge on or supplement the governance domain of traditional sovereign states. Under this design, multiple governance forums can play complementary roles, enhance co-operation and become more effective. This perspective allows for a considerably enhanced role for non-state actors, like the alliances of data protection authorities, the Commissioners' Conference or other civil society organizations (e.g. EPIC). A forum emerging from the institutionalization of inter-regime co-operation, as proposed here, would involve multiple stakeholders. Under current conditions of global governance, this seems a realistic prospect.

Now, in relation to substance: what does the suggested institutionalization look like? Would it be based on the much-debated and highly-anticipated EU-style regime? Or would it resemble the OECD Privacy Guidelines or the APEC Privacy Framework? Or would it incorporate the fundamentals of the Madrid Resolution? And—viewed through the lenses of legalization theory—where would it fall on the hard-vs.-soft-law spectrum? These questions provide room for speculation. No doubt, substituting any of the three existing privacy and data protection regimes into an international framework would be of minimum importance as these regimes are already evolving within their own frameworks. The more interesting proposition lies in a further evolution of the Madrid Resolution, which is drafted on the basis of the existing international consensus embodied in the existing international privacy and data protection regimes and other sources of international application.[603] The Madrid Resolution aims to

[603] See Madrid Resolution, *supra* note 253. The following reference in particular explicitly sets out this objective:

deliver an "effective and internationally uniform protection of privacy with regard to the processing of personal data"[604] by prescribing privacy principles. But at the same time it sets a higher standard for implementation and enforcement, by mandating a national supervisory authority with broad powers for both public and private sectors, and by supplementing the available judicial recourse, including added pecuniary damages along with civil and criminal measures. From a legalization-theoretic perspective, the obligation and delegation aspects of the Madrid Resolution aim at the higher end, which makes it closer to a hard-law formulation. That is where the theory implies serious doubts about its efficacy and the feasibility of its becoming a universal standard, as pursued by the Commissioners' Conference.[605] From a theoretical perspective, any efforts towards a hard-law form of the agreement are bound to imply higher sovereignty costs. This would likely encourage further transnational confrontations to protect national interests. In that light, the Madrid Resolution is very unlikely to be accepted by the US, or arguably by any other country with a soft-law national framework, as a *suo motto* template of a universal standard for privacy and personal data protection.

Therefore, the institutionalization of inter-regime co-operation proposed by the thesis would fall on the soft-law end of the obligation and delegation dimensions of legalization. Such an approach would not only offer the advantages of soft legalization enumerated in Chapter V,[606] but would also converge with Slaughter's theory about transgovernmental networks of global governance. The soft-to-hard-law transition is one of the more useful hypotheses about the interaction between hard and soft law interaction advanced by Shaffer & Pollack. A soft law may, under certain circumstances, translate into hard law. However, Abbott & Snidal also note

---

> The Working Group has drafted a Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, based on principles that are present in different instruments, guidelines or recommendations of international scope and that have received a broad consensus in their respective geographical, economic or legal areas.

[604] *Ibid*, see the purpose section of the Madrid Resolution.

[605] *Ibid* (It asserts in particular: "[t]he Joint Proposal demonstrates the feasibility of such standards, as a new step towards the development of a binding international instrument in due course").

[606] See Abbott & Snidal, *supra* note 525 at 445. Abbott & Snidal emphasize that "soft law should be attractive in proportion to the degree of divergence among the preferences and capacities of states, a condition that increases almost automatically as one moves from bilateral through regional to multilateral negotiations").

that it is not necessary that "all soft legalization is a way station to hard(er) legalization, or that hard legalization is the optimal form."[607] Under certain circumstances, soft law is more useful, particularly in the context of high sovereignty costs and contracting difficulties. "Hard law is probably more likely to evolve from soft law than from (utopian) plans to create hard law full-blown"[608]. At the same time, they provide a reminder that soft law has its own value in that it can provide a basis for efficient international contracts and help create normative covenants.[609] Raab observed that, "[n]ational or regional power differentials and differences of approach to privacy questions and their relation to other political objectives sought by countries or regions may be too much to bridge or suppress in favour of an overarching global framework.[610]

To reiterate, the thesis does not hope to develop a concrete blueprint for such an instrument, but to explore the prospects for one in the light of the theoretical approach adopted. The goal here is to make a generic case for institutionalization by rationalizing its viability in the light of the empirical evidence already presented. The former objective, by contrast, requires a new research project with further testing.

Another aspect to consider before closing the argument is to reflect on how the proposed solution helps in addressing some of our earlier observations about the three analytical components. First, the proposed institutionalization would likely be able to engage a wide range of stakeholders, including the data protection authorities and the Commissioners' Conference in particular. The data protection authorities could play an important role for their experience and expertise and be helpful in devising pragmatic policy solutions, which may help countries to learn and internalize new strategies and solutions in their domestic context. Importantly, the proposed approach will enhance the data protection authorities' role and prominence in national and international privacy and personal data governance. Second, the existing international privacy and data protection regimes may be able to evolve more efficiently both individually and collectively, which will further enhance the prospects not only

[607] *Ibid* at 447.

[608] *Ibid*.

[609] *Ibid* at 456.

[610] See Raab, "Networks for Regulation", *supra* note 26 at 209.

for harmonization of the member countries' national frameworks but also for strengthening inter-regime collaboration. Such a platform would minimize the divergence and maximize the convergence among national frameworks and international regimes. Third, the recommended approach would further engage the states in cordial and co-operative dialogue by providing a new platform for addressing and resolving differences and for developing norms and rules suited to specific needs and circumstances. Overall, the thesis conceives institutionalization as a potential win-win proposition, worthy of further consideration.

BIBLIOGRAPHY

1. **International privacy and data protection framework**
   A. OECD Privacy regime
   B. EU- COE 108 and Data Directive 95/46/EC
   C. APEC Privacy Framework
   D. US-EU Safe Harbor Agreement

2. **Privacy**
   A. Privacy and data protection- Conceptual framework
   B. Privacy and data protection- Transborder data flows context
   C. Privacy Enforcement Authorities/Data Protection Authorities

3. **Informing literature**
   A. Transgovernmental networks and global governance
   B. Regimes, institutions and legalization
   C. National interests and the resolution of transnational problems

4. **Analytical approach: Qualitative and Interdisciplinary (International law and international relations)**

5. **Online: Blogs, news sites and other online sources**

1. International privacy and data protection framework

A. OECD Privacy Regime

Primary documents:

Revised Privacy Guidelines (2013), online: OECD <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September 1980), online: OECD <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

Other related official documents:

OECD Privacy Framework (2013), online: OECD <http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2011), online: OECD iLibrary <http://www.oecdilibrary.org/docserver/download/5kgdpm9wg9xs.pdf?expires=1428689132&id=id&accname=guest&checksum=32D51EDC4E9E9CDD23A134784A0940F4>.

OECD Report on the Cross-Border Enforcement of Privacy Laws (2006), online: OECD <http://www.oecd.org/internet/ieconomy/37558845.pdf>.

OECD Ministerial Declaration on the Protection of Privacy on Global Networks (October 1998), online: OECD <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=109&InstrumentPID=106&Lang=en&Book=>.

The 30th Anniversary of the OECD Privacy Guidelines, online: OECD

<http://www.oecd.org/internet/ieconomy/the30thanniversaryoftheoecdprivacyguidelines.htm>.

Secondary materials:

Clarke, Roger. "Beyond the OECD Guidelines: Privacy Protection for the 21st Century", Department of Computer Science, Australian National University, online: Roger Clarke <http://www.rogerclarke.com/DV/PP21C.html>.

Greenleaf, Graham. "Global Data Privacy in a Networked World" in Brown I. ed, *Research Handbook on Governance of the internet (*Cheltenham: Edward Elgar, 2012) 2011-38.

———. "Global Data Privacy Laws: Forty Years of Acceleration" (2011) 112 Privacy Laws and Business International Report 11-17.

———. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" (2014) 23:1 J L & Info Science special edition: Privacy in the Social Networking World, online: SSRN
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877>.

Howard, Patrick P. "Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and the OECD Guidelines" (1981) 21 Jurimetrics 405.

Kirby, Michael. "Privacy Protection, a new Beginning: OECD Principles 20 Years on" (1999) 6:3 Privacy Law & Policy Reporter 25.

———. "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy" (2011) 1:1 International Data Privacy Law 6.

Wright, David, Hert, Paul De, Gutwirth, & Serge. "Are the OECD Guidelines at 30 Showing Their Age?" 54:2 Communications of the ACM 119-127, online: ACM DL Library <http://dl.acm.org/citation.cfm?id=1897848>.

B. EU COE 108 and Data Directive 95/46/EC

Primary documents:

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108 (2001), online: COE <http://conventions.coe .int/Treaty/EN/Treaties/HTML/181.htm>.

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (October 1995), online: Justice <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046>.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (1981), online: COE <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG>.

Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), online: COE <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 >.

Other related official documents:

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (2012), online: Justice <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011>.

European Commission's First Report on the Transposition of the Data Protection Directive (2003), online: Justice <http://ec.europa.eu/justice/data-protection/document/transposition/index_en.htm>.

European Commission, opinions and recommendations including decisions on adequacy assessments of the third country's national privacy and data protection frameworks, online: Justice <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>.

Status of implementation of Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data, online: Justice <http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm>.

Secondary materials:

Birnhack, Michael D. "The EU Data Protection Directive: An Engine of a Global Regime" (2008) 24:6 Computer L & Sec R 508.

De Hert, Paul. & Papakonstantinou Vagelis. "The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on Its Global Ambition" (2014) 30:6 Computer Law & Security Review 633.

Greenleaf, Graham. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108" (2012) 2:2 International Data Privacy Law; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299>.

———. "30 Years on: The Review of the Council of Europe Data Protection Convention 108" (2011) 27 Computer L & Sec R 223.

———. "Macao's EU-Influenced Personal Data Protection Act" (2008) 96 Privacy Laws & Business International Newsletter 21; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2027852>.

———. "Do Not Dismiss 'Adequacy': European Data Privacy Standards are Entrenched" (2011) 114 Privacy Laws & Business International Report 16; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2001825>.

———. “Strengthening and Modernising Council of Europe Data Privacy Convention 108” (2012) 117 Privacy Laws & Business International Report 21; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2118348>.

Peter, Ford. “Implementing the EC Directive on Data Protection - An Outside Perspective” (2003) 9:8 Privacy Law and Policy Reporter 141.

Poullet, Yves. “The Directive 95/46/EC: Ten Years After” (2006) 22 Computer L & Sec R 206.

Reding, Viviane. “The European Data Protection Framework for the Twenty-first Century” (2012) 2:3 International Data Privacy Law 119.

C. APEC Privacy Framework

Primary documents:

APEC Cross Border Privacy Rules System (2011), online: APEC <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx>.

APEC Cross-border Privacy Enforcement Arrangement (2010), online: APEC <http://mddb.apec.org/documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf>.

APEC Privacy Framework (2004), online: APEC <http://www.apec.org/Groups/Committee-on-Trade-and Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>.

Other related official documents

APEC-EU Common Referential for the Structure of the EU System of Binding Corporate Rules and APEC Cross Border Privacy Rules System (2014), online: APEC

<http://mddb.apec.org/Documents/2014/ECSG/ECSG1/14_ecsg1_013.pdf>.

APEC Data Privacy Pathfinder Projects (2007*),* online: APEC <http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx>.

Electronic Commerce Steering Group, Data Privacy Subgroup, online: APEC <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>.

Secondary materials:

Greenleaf, Graham. "Five Years of the APEC Privacy Framework: Failure or Promise?" (2009) 25 Computer L & Sec R 28; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2022907>.

———. "Asia-Pacific Developments in Information Privacy Law and its Interpretation" UNSW Law Research Paper No. 2007-5; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952578>.

———. "The APEC Privacy Initiative: 'OECD Lite' for the Asia-Pacific?" (2004) 71 Privacy Laws & Business International Report 16; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=510683>.

———. "APEC's Cross-Border Privacy Rules System: A House of Cards?" (2014) 128 Privacy Laws & Business International Report 27.

———. "APEC's CBPRs in Operation for Two Years: Low Take-Up, and Credibility Issues" (2014) 129 Privacy Laws & Business International Report 12; see online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468782>.

———. "A Tentative Start for Implementation Of APEC's Privacy Framework" (2005) 11:7 Privacy Law and Policy Reporter 188.

———. “APEC's Privacy Framework: A new Low Standard” (2005) 11:5 Privacy Law and Policy Reporter 121.

———. “APEC Privacy Principles Version 2: Not Quite so Lite, and NZ wants OECD Full Strength” (2003) 10:3 Privacy Law and Policy Reporter 45.

———. “Australia's APEC Privacy Initiative: The Pros and Cons of ‘OECD Lite’” (2003) 10:1 Privacy Law and Policy Reporter 1.

Tan, Johanna G. “A Comparative Study of the APEC Privacy Framework- A New Voice in the Data Protection Dialogue?” (2008) 3:1 Asian Journal of Comparative Law, online: Asian Journal of Comparative Law <http://www.degruyter.com/view/j/asjcl.2008.3.1/asjcl.2008.3.1.1071/asjcl.2008.3.1.1071.xml>.

D. US-EU Safe Harbor Agreement

Primary documents:

US-EU Safe Harbor Framework (2000), online: Export.gov <http://www.export.gov/safeharbor/eu/index.asp>.

US-EU Privacy Shield (2016), online: US Department of Commerce <https://www.commerce.gov/page/eu-us-privacy-shield>.

US-EU Umbrella Agreement (2016), online: EU Justice <http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>.

Maximillian Schrems v Data Protection Commissioner (Case C-362/14); Case online: Infocuria <http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=328696>

Other related official documents:

Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM/2013/0847), online: EUR-Lex <http://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1415704124887&uri=CELEX:52013DC0847>.

EU Commission decision on Safe Harbor agreement provides adequate protection (2000/520/EC), online: EUR-Lex <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0520>.

Secondary materials:

Cline, Jay. "Roadmap for an International Safe Harbor Framework" (2006) 20:3 Int'l Rev L Comp & Tech 361.

De Hert, P. & Bellanova, R. "Data Protection from a Transatlantic Perspective: The EU and U.S. Move Toward an International Data Protection Agreement?" (2008), online: Justice <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408320/IPOL-LIBE_ET(2008)408320_EN.pdf >.

Dhont J, Asinari, M.V.P & Poullet, Y. "Safe Harbour Decision Implementation Study" (2004), online: Justice <http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf>.

Farrell, Henry. "Constructing the International Foundations of E-Commerce-The EU-U.S. Safe Harbor Arrangement" (2003) 57:2 International Organization 277.

Gonzalez-Fuster, G. De Hert, P. & Gutwirth, S., "SWIFT and the Vulnerability of Transnational Data Transfers" (2008) 22:1/2 Int'l Rev L Comp & Tech 191.

Hustinx, Peter. European Union's Data Protection Supervisor, Opinion on the US-EU Data Exchange Agreement (2008), online: EDPS <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf>.

Korff, Douwe. "EU-US Umbrella Data Protection Agreement: Detailed Analysis" (14 October 2015), online: European Area of Freedom Security & Justice <http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/>.

Lee, Dave. "Apple v FBI: US Debates a World without Privacy" (2 March 2016), online: BBC <http://www.bbc.com/news/technology-35704103>.

Leetaru, Kalev. "Why The Apple Versus FBI Debate Matters In A Globalized World" (2 March 2016), online: Forbes <http://www.forbes.com/sites/kalevleetaru/2016/03/02/why-the-apple-versus-fbi-debate-matters-in-a-globalized-world/#5c93fdda2639>.

Long, WJ, & MP Quek. "Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise" (2002) 9:3 Journal of European Public Policy 325.

Shaffer, Gregory. "Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements" (2002): 9 Colum J Eur L 429.

Stevens, Christopher & Holland, Stephen. "How (and Why) Safe Harbor needs to be Reformed" (26 August 2014), online: IAAP <https://iapp.org/news/a/on-why-safe-harbor-needs-to-be-reformed>.

Weber, Rolf H. "Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives" (2013) 3:2 International Data Privacy Law 117.

Weiss Martin A. & Archick, Kristin. "U.S.-EU Data Privacy: From Safe Harbor to Privacy

Shield" (12 February 2016), online: US Congress Research Services <https://www.fas.org/sgp/crs/misc/R44257.pdf>.

Wolf, Christopher. "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-border EU-U.S. Data Transfers" (2013) 43 Wash UJL & Pol'y 227.

2. Privacy

A. Privacy and data protection- Conceptual framework

Books:

Agre, Philip E. & Rotenberg, Marc. eds, *Technology and Privacy: The New Landscape* (Cambridge, MA: MIT Press, 1998).

Bennett, Colin J. & Grant, Rebecca. eds, *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

Bygrave, Lee A. *Data Privacy Law: An International Perspective* (Oxford, UK: Oxford University Press, 2014).

Cate, Fred H. *Privacy in the Information Age* (Washington, D.C.: Brookings Institution Press, 1997).

Greenawalt, Kent. "Privacy and Its Legal Protection" (1974) 2:3 The Hastings Center Studies, The Future of Individualism 55-67.

Solove, Daniel J., Rotenberg, Marc & Schwartz, Paul M. eds, *Information Privacy Law*, 2nd ed (New York: Aspen Publishers, 2006).

Westin, Alan F. *Privacy and Freedom* (New York: Athenaeum, 1967).

Articles:

Chlapowski, Francis S. "The Constitutional Protection of Informational Privacy" (1991) 71 BUL Rev 133.

Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects" (2009) 25.4 Computer Law and Security Review 307.

Gavison, Ruth. "Privacy and the Limits of Law" (1980) 89 Yale LJ 421.

Michael, Kirby, "Privacy Protection- A New Beginning?" High Court of Australia, online: Speeches <http://www.hcourt.gov.au/publications_05.html#MichaelKirby>.

Phillips, Bruce. "Privacy in the Information Age: an Oxymoron?" (26 January 1995), online: OPC Archived Speeches <https://www.priv.gc.ca/media/spd/archive/02_05_a_950126_e.asp>.

Reidenberg, Joel R. "Privacy in the Information Economy: A Fortress or a Frontier for Individual Rights?" (1991) 44 Fed Comm LJ 195.

Rotenberg, Mark. "On International Privacy: A Path Forward for the US and Europe" (15 June 2014), online: Harvard International Review <http://hir.harvard.edu/on-international-privacy-a-path-forward-for-the-us-and-europe/>.

Samuelson, Pamela J. "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy" (1999) 87 Cal L Rev 751.

Schwartz, Paul M. "Charting a Privacy Research Agenda: Responses, Agreements, and Reflections" (2000) 32 Conn L Rev 929.

Schwartz, Paul M. "Privacy and Democracy in Cyberspace" (1999) 52 Vand L Rev 1609.

Simitis, Spiros. “Reviewing Privacy in an Information Society” (1987) 135:3 U Pa L Rev 707.

Solove, Daniel J. “Conceptualizing Privacy” (2002) 90 Cal L Rev 1088.

Warren, Samuel D. & Brandeis, Louis D. “The Right to Privacy” (1890) 4 Harv L Rev 193.

Westin, Alan F. “Social and Political Dimensions of Privacy” (2003) 59:2 Journal of Social Issues 431.

B. Privacy and data protection- Transborder data flows context

Books:

Banisar, David & Davies, Simon. “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments” (1999) 18 J Marshall J Computer & Info L 1.

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

Bennett, Colin J. & Raab, Charles. *The Governance of Privacy: Policy Instruments in Global Perspective* (Aldershot: Ashgate Press, 2003).

Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989).

Heisenberg, Dorothee & Fandel, Marie-Helene. “Projecting EU Regime Abroad: The EU Data Protection Directive as Global Standard” in Sandra Braman, eds, *The Emergent Global Information Policy Regime* (New York: Palgrave Macmillan, 2004).

Heisenberg, Dorothee. *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (London: Lynne Rienner Publishers, 2005).

Articles:

Abrams, Richard M. "The End of Privacy: 9/11 and the Ascendancy of the Surveillance State" Japan Policy Research Institute, Working Paper No. 122 (January 2014), online: jpri.org <http://www.jpri.org/publications/workingpapers/wp122.html>.

Cate, Fred H. "Global Information Policymaking and Domestic Law" (1994) Ind J Global Legal Stud 467.

Cate, Fred H. "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33 Ind L Rev 173.

Bennett, Colin J. "Review Article: What is Policy Convergence and What Causes it?" (1991) 21:2 British Journal of Political Science 215.

———. "Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States" (1988) 1:4 Governance 415.

———. "The Geo-Politics of Personal Data", (December 14, 2012), online: Harvard International Review <http://hir.harvard.edu/archives/3016>.

EPIC et al, Development and Implementation of Cross-border Privacy Rules in the Asia Pacific Economic Co-operation Group (APEC) submission to the Department of Commerce, International Trade Administration, online: EPIC <http://www.epic.org/privacy/intl/apec_cmts.pdf>.

Francis S. Chlapowski, Francis S. "The Constitutional Protection of Informational Privacy" (1991) 71 BUL Rev 133.

Gellman, Robert. “Can Privacy be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules” (1996) 41 Vill L Rev 129.

———. “Fragmented, Incomplete, and Discontinuous: the Failure of Federal Privacy Regulatory Proposals and Institutions” (1993) VI Software LJ 199.

Greenleaf, Graham. “Global Data Privacy Laws 2013: 99 Countries and Counting” (2013) 123 Privacy Laws & Business International Report 10; also available online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305882>.

Kobrin, Stephen J. “The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance” (2002) The Wharton School, University of Pennsylvania, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=349561>.

Ohm, Paul. “Don’t Build a Database of Ruin” (23 August 2012), online: Harvard Business Review <https://hbr.org/2012/08/dont-build-a-database-of-ruin>.

Raab, Charles. “Information Privacy: Networks of Regulation at the Sub-global Level“ (2010) 1:3 Global Policy Journal 291.

Reidenberg, Joel R. “Resolving Conflicting International Data Privacy Rules in Cyberspace” (2000) 52 Stan L Rev 1315.

Salbu, Steven R. “The European Union Data Privacy Directive and International Relations” (2002) 35 Vand J Transnat'l L 655.

Schwartz, Paul M. “European Data Protection Law and Restrictions on International Data Flows” (1995) 80 Iowa L Rev 471.

Shaffer, Gregory. “Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards” (2000) Yale J Int’l L 1.

Swire, Peter P. “Of Elephants, Mice, and Privacy: International Choice of Law and the Internet” (1998) 32 Int'l Law 991.

Simitis, Spiros. “From the Market to the Polis: The EU Directive on the Protection of Personal Data” (1995) 80 Iowa L Rev 445.

Virginia, Haufler and Randi, Bessette. “Why There is no International Regime for Information Privacy Protection” (2001) 2:1 International Studies Perspective 69.

Vries, Will Thomas De. “Protecting Privacy in the Digital Age” (2003) 18 Berkeley Tech LJ 283.

C. Privacy Enforcement Authorities/Data Protection Authorities

Websites and official documents:

Asia Pacific Privacy Authorities (APPA), online: APPA <http://www.appaforum.org>.

Global Privacy Enforcement Network (GPEN), online: GPEN <https://www.privacyenforcement.net>.

27th International Conference on Privacy and Personal Data Protection Commissioners, Montreux, Switzerland (2005), online: Privacy Conference <http://www.privacyconference2005.org/>.

28th International Conference on Privacy and Personal Data Protection Commissioners, London, UK (2006), online: Privacy Conference <http://www.privacyconference2006.co.uk/>.

29th International Conference on Privacy and Personal Data Protection Commissioners, Montreal, Canada (2007), online: Privacy Conference

<http://www.privacyconference2007.gc.ca/>.

30th International Conference on Privacy and Personal Data Protection Commissioners, Strasbourg, France (2008), online: Privacy Conference <http://www.justice.gov.il/PrivacyGenerations/adopted.htm>.

31st International Conference on Privacy and Personal Data Protection Commissioners, Madrid, Spain (2009), online: Privacy Conference <www.privacyconference2009.org/home/index-iden-idweb.html>

32nd International Conference on Privacy and Personal Data Protection Commissioners, Jerusalem, Israel (2010), online: Privacy Conference <http://www.justice.gov.il/PrivacyGenerations>.

33rd International Conference on Privacy and Personal Data Protection Commissioners, Mexico City, Mexico (2011), online: Privacy Conference <http://privacyconference2011.org/index.php?lang=Eng>.

34th International Conference on Privacy and Personal Data Protection Commissioners, Punta del Este, Uruguay (2012), online: Privacy Conference <http://privacyconference2012.org/english/>.

35th International Conference on Privacy and Personal Data Protection Commissioners, Warsaw, Poland (2013), online: Privacy Conference <https://privacyconference2013.org/>.

36th International Conference on Privacy and Personal Data Protection Commissioners, Mauritius (2014), online: Privacy Conference <http://www.privacyconference2014.org>.

37th International Conference on Privacy and Personal Data Protection Commissioners, Amsterdam (2015), online: Privacy Conference <http://www.apc2015.net/content/amsterdam-privacy-week>.

Secondary materials:

Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008).

———. *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2006).

———. & Raab, Charles D. "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas" (2003) 46 Canadian Public Administration 218.

———. "Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies" (2011) 13 Journal of Comparative Policy Analysis 2.

Bygrave, Lee. "Privacy Protection in a Global Context– A Comparative Overview" (2004) 47 Scand Stud L 319.

Greenleaf, Graham. "Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience" (2012) 28:1/2 Computer L & Sec R; see online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1971627>.

———"Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners" in Paul Roth, ed*, Privacy law and Policy Review in New Zealand* (Wellington, New Zealand: Butterworths-LexisNexis 2004).

Newman, Abraham L. "Transatlantic Flight Fights: Multi-level Governance, Actor Entrepreneurship and International Anti-terrorism Co-operation" (2011) 18:4 Review of International Political Economy 481.

———. “Watching the Watchers: Transgovernmental Implementation of Data Privacy Policy in Europe” (2011) 13:2 Journal of Comparative Policy Analysis 181.

———“Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive” (2008) 62:1 International Organization 103.

Newman, Abraham L. & Bach, David. “The Domestic Drivers of Transgovernmental Regulatory Co-operation” (2014) 8:4 Regulation and Governance 395.

———. “The European Union as a Hardening Agent: Soft law and the Diffusion of Financial Regulation” (2014) 21:3 Journal of European Public Policy 430.

———. “Transgovernmental Networks and Domestic Policy Convergence: Evidence from Insider Trading Regulation” (2010) 64:3 International Organization 505.

Newman, Abraham L. & Farrell, Henry. “Domestic Institutions Beyond the Nation State: Charting the New Interdependence Approach” (2014) 66:2 World Politics 331.

———. “The New Politics of Interdependence: Cross-National Layering in Trans-atlantics Regulatory Disputes” (2015) 48:4 Comparative Political Studies 497.

Newman, Abraham L. & Eberlein, Burkard. “Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union” (2008) 21:1 Governance 25.

Newman, Abraham L. & Zaring, David. “Regulatory Networks: Power, Legitimacy, and Compliance,” in Dunoff, Jeffery & Pollack, Mark. eds, *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (Cambridge, MA: Cambridge University Press, 2012).

Raab, Charles D. “Networks for Regulation: Privacy Commissioners in a Changing World” (2011) 13:2 Journal of Comparative Policy Analysis 195.

———. "Beyond Activism: Research Perspectives on Privacy" (2008) Tilburg University Legal Studies Working Paper No. 004/2008 (TILT Law & Technology Working Paper Series No. 007/2008), online: SSRN <http://ssrn.com/abstract=1096562>.

———. & Koops, Bert-Jaap. "Privacy Actors, Performances and the Future of Privacy Protection" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cecile de Terwangne & Sjaak Nouwt. eds, *Reinventing Data Protection*? (Dordrecht: Springer, 2009).

3. Informing Literature

A. Transgovernmental networks and global governance

Avant, Deborah D., Finnemore, Martha & Sell, Susan K. eds, *Who Governs the Globe?* (Cambridge, UK: Cambridge University Press, 2010).

Drezner, Daniel. "The Global Governance of the Internet: Bringing the State Back In" (2004) 119 Political Science Quarterly 477.

Ernst, Hass B. "Is there a Hole in the Whole? Knowledge, Technology, Interdependence, and Construction of International Regimes" (1975) 29:3 International Organization 827.

Haas, Peter. "Epistemic Communities and International Policy Coordination" (1992) 66:1 International Organization 1.

Hall, Rodney B. & Biersteker, Thomas J. eds, *The Emergence of Private Authority in Global Governance* (Cambridge, UK: Cambridge University Press, 2002).

Held, David & Anthony, McGrew. "Globalization" (1999) 5:4 Global Governance 483.

———. *Democracy and the Global Order* (Stanford, CA: Stanford University Press, 1995).

Joel, Redienberg. “Governing Networking and Rule-Making in Cyberspace” (1996) 45 Emory LJ 911.

———. "Resolving Conflicting International Data Privacy Rules in Cyberspace” (2000) 52.5 Stan L Rev 1315.

Keohane, Robert O., *After Hegemony: Co-operation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 1984).

———. “The Legitimacy of Global Governance Institutions” (2006) 20:4 Ethics and International Affairs 405.

———. & Nye, Joseph S. “Power and Interdependence in the Information Age” (1998) 77:5 Foreign Affairs 81.

———. “Governance in a Partially Globalized World” (2000) 95 American Political Science Review 1.

Kobrin, Stephen. “Territoriality and the Governance of Cyberspace” (2001) 32:4 Journal of International Business Studies 687.

Krasner, Stephen D. “Globalization and Sovereignty,” in Smith, David A., Solinger, Dorothy J. & Topik, Steven C. eds, *States and Sovereignty in the Global Economy* (New York: Rutledge, 1999).

Manuel, Castells. ed, *The Rise of the Network Society* (Malden, MA: Blackwell Publishers, 2000).

Margret, E. Keck & Kathryn, Sikkink. *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998).

Milner, Helen & Moravcsik, Andrew. eds, *Power, Interdependence and Non-state Actors in World Politics* (Princeton, NJ: Princeton University Press, 2009).

Nye, Joseph S. “The Regime Complex for Managing Global Cyber Activities”, Global Commission on Internet Governance Paper Series No. 1, online: CIGI <https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities>.

Price, Richard. “Transnational Civil Society and Advocacy in World Politics” (2003) 55:4 World Politics 579.

Roderick, Dani. *Has Globalization Gone Too Far?* (Washington, D.C.: Institute of International Economics, 1997).

Rosenau, James. “Governance in the Twenty-First Century” (1995) 1:1 Global Governance 14.

Ruggie, John. “Reconstituting the Global Public Domain— Issues, Actors and Practices” (2004) 10:4 EJIL 499.

Slaughter, Anne-Marie & Hale, Thomas N. “Transgovernmental Networks” in Mark Bevir, ed, *SAGE Handbook of Governance* (London, UK: Sage, 2010) 342.

———. & Zaring. David. “Networking Goes International: An Update” (2006) 2 Annual Review of Law and Social Science 211.

———. “Disaggregated Sovereignty: Toward the Public Accountability of Global Government Networks” (2004) 39:2 Government and Opposition 159.

———, “Global Government Networks, Global Information Agencies, and Disaggregated Democracy” (2003) 24 Mich J Int'l L 1041.

———“Agencies on the Loose? Holding Government Networks Accountable” in George A. Bermann, Matthias Herdegen & Peter Lindseth, eds, *Transatlantic Regulatory Co-operation* (Oxford: Oxford University Press, 2001).

———. “Sovereignty and Power in a Networked World Order” (2004) 40 Stan J Int’l L 283.

———. *A New World Order* (Princeton, NJ: Princeton University Press, 2004).

Wolf, Martin. "Will the Nation-state Survive Globalization?" (2000) 80:1 Foreign Affairs 178.

B. Regimes, institutions and legalization

Abbott, Kenneth W., et al, "The Concept of Legalization" (2000) 54:3 International Organization 401.

———. "International 'Standards' and International Governance" (2001) 8 Journal of European Public Policy 345.

———. "International Relations Theory, International Law, and the Regime Governing Atrocities in Internal Conflicts" (1999) 93:2 AJIL 361.

———. "Why State Act through Formal International Organization" (1998) 42:1 Journal of Conflict Resolution 3.

———. & Snidal, Duncan. "Hard and Soft Law in International Governance" (2000) 54:3 International Organization 421.

Bendrath, Ralf. "The Return of the State in Cyberspace: The Hybrid Regulation of Global Data Protection" in Myriam Dunn, Sai Felicia Krishna-Hensel & Victor Mauer, eds, *The Resurgence of the State, Trends and Process in Cyberspace Governance* (Hampshire, England: Ashgate Publication 2007) at 135.

Haggard, Stephan & Simmons, Beth A. "Theories of International Regimes" (1987) 41:3 International Organization 491.

Keohane, Robert O. *Power and Governance in a Partially Globalized World* (New York: Rutledge, 2002).

———. "The Demand for International Regimes" (1982) 36:2 International Organization 325.

———. *After Hegemony: Co-operation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 1984).

Krasner, Stephen. "Structural Causes and Regime Consequences: Regimes as Intervening Variables" (1982) 36:2 International Organization 185.

———. "Global Communications and National Powers: Life on the Pareto Frontier" (1991) 43:3 World Politics 336.

Martin, Lisa L. & Simmons, Beth A. "Theories and Empirical Studies of International Institutions" (1998) 52:4 International Organization 729.

Shaffer, Gregory C. & Pollack, Mark A. "Hard Versus Soft Law in International Security" (2011) 52:4 BCL Rev 1147 [Shaffer & Pollack] at 1147. Also available, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1786836>.

Slaughter, Anne-Marie. "International Law and International Relations Theory: A Prospectus" in Eyal Benevisti & Moshe Hirsch, eds, *The Impact of International Law on International Co-operation* (New York: Cambridge University Press, 2004).

———. "Sovereignty and Power in a Networked World Order" (2004) 40 Stan J Int'l L 283.

———. et al, eds, *Legalization and World Politics* (Massachusetts: MIT Press, 2001).

———. et al, eds, Legalization and World Politics: A Special Issue of International Organization (2000) 54 International Organization 1.

Young, Oran R. "Review Article, International Regimes: Toward a New Theory of Institutions" (1986) 39:1 World Politics 104.

C. National interest and resolution of transnational problems

Kratochwil, Friedrich. "On the Notion of 'interest' in International Relations" (1982) 36:1

International Organization 1.

Nincic, Miroslav. “The National Interest and Its Interpretation” (1999) 61:1 The Review of Politics 29.

Rochester, Martin J. “The ‘National Interest’ and Contemporary World Politics” (1978) 40.1 The Review of Politics 77.

Rosenau, James. “National Interest” in International Encyclopedia of the Social Sciences (1968), online: Encyclopedia.com <http://www.encyclopedia.com/doc/1G2-3045000855.html>.

Scott, Burchill. *The National Interest in International Relations Theory* (Houndmills, New York: Palgrave Macmillan, 2005).

Tonelson, Alan. “What is the National Interest?” (1991) 268:1 The Atlantic Monthly 35.

Williams, Michael. “What Is the National Interest? The Neoconservative Challenge in IR Theory” (2005) 11:3 European Journal of International Relations 307.

4. Analytical approach: Qualitative and interdisciplinary (International law and international relations)

Abbott, Kenneth W. “Modern International Relations Theory: A Prospectus for International Lawyers” (1989) 14 Yale J Int'l L 335.

———. “Symposium on Method in International Law: International Relations Theory, International Law, and the Regime Governing Atrocities in Internal Conflicts” (1999) 93 AJIL 361.

———. & Snidal Duncan, “Law, Legalization, and Politics: An Agenda for the Next Generation of IR/IL Scholars” in Jeffrey Dunoff & Mark Pollack, eds, *Interdisciplinary*

Perspectives on International Law and International Relations: The State of the Art (New York: Cambridge University Press, 2013).

Beck, Robert J. "International Law and International Relations: The Prospects for Interdisciplinary Collaboration" (1995) 1 J Int'l Legal Stud 119.

———. "International Law and International Relations: A Scheme for Classifying their Literatures" (2000) 94 Proceedings of the Annual Meeting, ASIL 211.

Harold Hongju Koh, Abbott, Kenneth W. & Young, Oran R. "Elements of a Joint Discipline" (1992) 86 Proceedings of the Annual Meeting, ASIL 167.

Joyner, Christopher C. "Review: International Law is, as International Relations Theory Does?" (2006) 100:1 AJIL 248.

Keohane, Robert O. "International Relations and International Law: Two Optics" (1997) 38:2 Harv Int'l LJ 487.

King, Garry, Keohane, Robert O. & Sidney Verba, *Designing Social Inquiry* (Princeton, NJ: Princeton University Press, 1996).

Ratner Steven R. & Slaughter, Anne-Marie. eds, "Symposium on Method in International Law: A Special Issue of the AJIL" (1999) 93 AJIL 291.

Slaughter, Anne-Marie. "A Liberal Theory of International Law", Proceedings of the 94th Annual Meeting of ASIL 2000.

———. "International law and International Relations Theory: a New Generation of Interdisciplinary Scholarship" (1998) 92 AJIL 367.

———. "International Law and International Relations Theory: Twenty Years Later" in Dunoff, Jeffrey L. & Pollack, Mark A. eds, *Interdisciplinary Perspectives on International*

Law and International Relations: The State of the Art (Cambridge, UK: Cambridge University Press, 2012).

———. "International Law and International Relations Theory: A Prospectus" in Benevisti, Eyal & Hirsch, Moshe. eds, *The Impact of International Law on International Co-operation* (Cambridge, UK: Cambridge University Press, 2004).

———. & Raustiala Kal. "International Law, International Relations and Compliance" in Carlnaes, Walter, Risse, Thomas & Simmons, Beth. eds, *Handbook of International Relations* (London, UK: Sage, 2001).

Slaughter, Anne-Marie Burley. "International Law and International Relations Theory: A Dual Agenda" (1993) 87 AJIL. 205.

5. Online: Blogs and other online sources

Anne-Marie Slaughter, online: Slaughter <http://scholar.princeton.edu/slaughter>.

Colin J. Bennett, online: Bennett <http://www.colinbennett.ca>.

Electronic Frontier Foundation, online: EFF <https://www.eff.org>.

Electronic Privacy Information Center, online: EPIC <https://epic.org>.

Michael Geist, online: Geist <http://www.michaelgeist.ca>.