AFFAIRES GENERALES ET POLITIQUE
GENERAL AFFAIRS AND POLICY

Doc. prél. No 13
Prel. Doc. No 13

mars / March 2010

HccH
HAGUE CONFERENCE ON
PRIVATE INTERNATIONAL LAW
CONFÉRENCE DE LA HAYE
DE DROIT INTERNATIONAL PRIVÉ

FLUX TRANSFRONTALIERS DE DONNÉES ET PROTECTION DE LA VIE PRIVÉE

Note établie par le Bureau Permanent

* * *

CROSS-BORDER DATA FLOWS AND PROTECTION OF PRIVACY

Note submitted by the Permanent Bureau

Document préliminaire No 13 de mars 2010 à l'intention
du Conseil d'avril 2010 sur les affaires générales et la politique de la Conférence

Preliminary Document No 13 of March 2010 for the attention
of the Council of April 2010 on General Affairs and Policy of the Conference

Permanent Bureau | *Bureau Permanent*
6, Scheveningseweg 2517 KT The Hague | *La Haye* The Netherlands | *Pays-Bas*
telephone | *téléphone* +31 (70) 363 3303 fax | *télécopieur* +31 (70) 360 4867
e-mail | *courriel* secretariat@hcch.net website | *site internet* http://www.hcch.net

FLUX TRANSFRONTALIERS DE DONNÉES ET PROTECTION DE LA VIE PRIVÉE

Note établie par le Bureau Permanent

* * *

CROSS-BORDER DATA FLOWS AND PROTECTION OF PRIVACY

Note submitted by the Permanent Bureau

I. Introduction

1. The number of cross-border civil and commercial matters involving personal data issues are increasing as globalisation and e-commerce continue to grow. As a result, the need for a consistent and predictable regime for the application of international data transfer rules is a recurrent issue at the domestic, regional and international levels. The Permanent Bureau's aim in drafting this Note is to report on recent developments in this area.

2. Cross-border data transfers are intrinsic to personal and professional relationships throughout the world, particularly when the ubiquitous nature of the Internet is taken into account. The added convenience and efficiency resulting from global data flows also increases the risk to individuals' privacy. Protecting privacy in a global environment depends on cross-border co-operation. Although the need for effective enforcement and co-operation has been duly noted for many years, there is now renewed interest in working at the international level to address outstanding challenges in a world where trans-border data flows are widespread and continuous. Protection of privacy in an international context has become increasingly complex, and has become inherently linked with other important global issues, such as human rights, security, trade and development.[1]

3. As the issue has grown in scale and complexity, States, international organisations and other stakeholders are often uncertain of the best way to manage complex cross-border data transfers and to respond to data protection challenges. Quite naturally, many governments tend to favour unilateral procedures, but it is increasingly apparent that international data transfers are driven by global forces, and there is growing awareness that international co-operation is essential to effectively secure more legal certainty in this area.

4. Protection of privacy in respect of cross-border data transfers has always been a matter of interest in the development, implementation and application of Hague Conventions.

5. On the one hand, data protection laws and regulations affect potential solutions to private international law issues that rely on transfers of data across borders, and the willingness of governments to embrace these solutions. From the 1990s onward, the Hague Conference's Conventions and their implementing instruments seek indeed to ensure that international transfers of data occur in accordance with data protection obligations (*e.g.*, Articles 30-31 of the 1993 Adoption Convention or Articles 38–40 of the 2007 Child Support Convention). On the other hand, the practical implementation of some Hague Conventions resulting in the international transfer of personal data has given rise to challenging questions about their relationship with data protection regimes (*e.g.*, collecting evidence abroad for litigation purposes and the debate about the mandatory nature of the 1970 Hague Evidence Convention).[2]

---

[1] See "The Data Deluge: Businesses, governments and society are only starting to tap its vast potential", *The Economist* (25 February 2010), p. 11; "A special report on managing information: Data, data everywhere", *The Economist* (25 February 2010), p. 16.

[2] *See, e.g.,* Working Document No 1/2009 of Data Protection Working Party on pre-trial discovery for cross-border civil litigation. The conclusion in this document is in line with that of the Hague Conference Special Commission on the practical operation of the Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions in 2009: the effective operation of the Convention provides a mechanism for effective cross-border co-operation with a view to transferring personal (or other) data. Difficulties may arise, however, where cross-border evidence is sought beyond the scope of the Convention.

6. The work of the Hague Conference is, therefore, inextricably linked to the current debate on diverging legal and regulatory requirements applicable to cross-border data flows, particularly as the matter relates to civil and commercial matters. Against this background, the Permanent Bureau was very pleased to be invited by the Spanish Data Protection Agency to attend the most recent International Conference of Data Protection Commissioners, held in Madrid (Spain) from 4 to 6 November 2009, and to give a presentation at the session on "Determining the applicable law in a global world". This Note reports on a very interesting exchange of views in Madrid and in further consultations with a number of stakeholders about the possible techniques for bringing about an international data protection framework. As a preliminary matter, a succinct overview of recent international data protection initiatives that in some way relate to private international law is provided below as background for the current state of affairs in this area.

II. A decade of international data protection in a nutshell

7. It is no less than a decade ago that the Permanent Bureau last submitted a document on the issue of cross-border data protection in the context of private international law. Preliminary Document No 7 of April 2000, "Electronic Data Interchange, Internet and Electronic Commerce", acknowledged the groundbreaking work of a number of international organisations with regard to the protection of privacy in connection with trans-boundary data flows and suggested some avenues for future Hague Conference work.[3] It is unnecessary to repeat here the overview of relevant work completed by the Organisation for Economic Cooperation and Development (OECD), the Council of Europe and the European Union described in that document. In light of the vast range of activities ongoing at that time in different public and private circles, the study was confined "to the work of organizations concerned with the unification of private law *stricto sensu*".[4] In addition, it was suggested that the protection of privacy in an international context would require several components, *i.e.,* not only a system of conflicts of law but also an adequate dispute settlement mechanism and a method permitting "a degree of monitoring and supervision of data exploitation activities".[5] It should be noted that the topic was studied from the specific angle of electronic data transfers and, accordingly, was retained on the Agenda of the Conference under a more general title, *i.e.*, "Questions of private international law raised by the information society, including electronic commerce". Last year, the Council agreed to complete the reference by a specific mention to "e-justice".

8. The OECD, the Council of Europe and the European Union, together with many other international and regional entities, have continued with their important work on international data protection. In addition to pioneering instruments such as Convention 108 of the Council of Europe[6] and the OECD "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of

[3] See Hague Conference, "Electronic Data Interchange, Internet and Electronic Commerce", Prel. Doc No 7 of April 2000 for the attention of the Special Commission of May 2000 on general affairs and policy of the Conference. *See also* Recommendations of the Geneva Roundtable on Electronic Commerce and Applicable Law (September 1999). In the matter of data protection, the Roundtable recognised that data collection, personal data included, and processing thereof are inherent to electronic commerce. It further stated that the dichotomy between systems which do not accept general standards and those which require a rigid *a priori* framework for the collection and transfer of data should be avoided. Furthermore, it was suggested to carry out a study on the most relevant system of applicable law which would also allow a greater role to self-regulation and model contracts such as those proposed by the ICC and in line with the principles recommended by the Council of Europe.

[4] *Ibid*., p. 285.

[5] *Ibid*., p. 299.

[6] Council of Europe (1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, Council of Europe, European Treaty Series No 108.

Personal Data" (1980),[7] more recent regional instruments such as the European Union Data Protection Directive (1995),[8] the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2005),[9] the Asia-Pacific Privacy (APP) Charter Initiative (developed by an NGO group of experts in 2003; as of early 2010, a second version of the Charter had not yet been released for public comment)[10] and the Ibero-American Meetings[11] all attempt to provide more legal certainty in the legal framework applicable to cross-border data transfers.[12]

9. There have also been attempts to address trans-border data protection through bilateral agreements. The EU-US High Level Contact Group, for example, has been working on a transatlantic agreement with common principles for privacy and data protection.[13] It should be noted, however, that this bilateral agreement was created for purposes of combating terrorism and other law enforcement purposes and does little in the way of addressing cross-border data transfer issues in the commercial or civil context. It is a notable development, however, because it provides an example of two different privacy regimes (the EU and U.S.) attempting to identify common substantive principles for cross-border data flows. The goal of the High Level Contact Group was to build on recent trans-Atlantic events, which have included the conclusion of international agreements between the United States and the European Union governing Extradition and Mutual Legal Assistance (2003), and Passenger Name Record (PNR) data (2007), as well as agreements governing personal data exchange between the United States and Europol (2002) and Eurojust (2006).

---

[7] *Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data* (23 September 1980), Paris, OECD, ISBN 92-64-19719-2, hereinafter referred to as "OECD Guidelines".

[8] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("EU Directive"). Article 4 of the EU Directive refers to applicable law but fails to provide much certainty in practice.

[9] *APEC Privacy Framework* (2005), Singapore, APEC Secretariat, ISBN I 981-05-4471-5. The APEC Privacy Framework aims to promote a consistent approach to information privacy protection, to avoid the creation of unnecessary barriers to information flows and to remove impediments to trade across APEC member economies. The Framework also provides technical assistance to APEC economies that have not addressed privacy from a regulatory or policy perspective. For more information, see www.apec.org, then "Committee on Trade and Investment", "Electronic Commerce Steering Group" and then "APEC Privacy Framework." The APEC Member Economies include Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Viet Nam.

[10] G. Greenleaf & N. Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0* (2003), PRIV. L. RES. 1, Baker & McKenzie Cyberspace Law and Policy Centre, 3 September 2003.

[11] Since 2002, the Ibero-American meetings have been held annually to address matters that are highly relevant in the sphere of personal data protection, such as the latest regulatory and legal advances related to privacy and data protection in Latin American countries, international data transfers to Latin America, the processing of personal data of minors, or data processing in the sphere of scientific research, among others. The Ibero-American Data Protection Network (RIPD) adopted a statement during its sixth meeting held in Columbia in May 2008 appealing to the international conferences relating to data protection and privacy, regardless of their geographical scope, to continue their efforts to adopt a common legal instrument.

[12] It is also important to note the work of the International Conference of Data Protection and Privacy Commissioners who have held meetings and issued statements urging a more globalised approach to data protection and privacy for the last several years. *See, e.g.*, *Montreux Declaration: The protection of personal data and privacy in a globalised world: a universal right respecting diversities* (2005), Montreux, Twenty-Seventh International Conference of Data Protection and Privacy Commissioners. Subsequent conferences were held in 2006 (London), 2007 (Montreal), 2008 (Strasbourg), and 2009 (Madrid).

[13] See United States Mission to the European Union, *U.S., EU Issue Statement on Common Data Privacy and Protection Principles* (12 December 2008).

III. Focus on co-ordination techniques

10. The focus for the various initiatives mentioned above lies with the substantive approximation of privacy and data protection laws. The possible co-ordination of these laws by means of private international law mechanisms is yet another specific technique to be considered. As early as 1981, the Explanatory Memorandum to the OECD Guidelines contemplated such an approach but recognised that a solution based more on private international law would be very difficult.[14] The Expert Group drafting the Explanatory Memorandum therefore decided that in light of rapidly changing technology and the non-binding nature of the Guidelines, it would do nothing beyond issuing a statement which merely signaled the existence of these issues, which Member States should try to eventually resolve.[15]

11. Almost 30 years later, States have made relatively little progress to identify an acceptable solution to cross-border transactions involving personal data. It is, admittedly a very difficult issue that has not become easier to address over time but is rather becoming more acute in light of the growing importance of data processing in the global economy. There is, therefore, a renewed interest for these issues, as some examples provided below illustrate.

A. Cross-border conflicts in practice

12. Companies operating globally would clearly benefit from a clearer regime in this area. For example, in *Privacy Commissioner of Canada v. SWIFT* (April 2, 2007), it was alleged that SWIFT, a company established primarily in Belgium and the United States, inappropriately disclosed to the US Treasury personal information originating from or transferred to Canadian financial institutions. The Canadian Privacy Commissioner determined that SWIFT was subject to the Personal Information Protection and Electronic Documents Act (PIPEDA) because the organisation operated in and was connected in a substantial way to Canada. She noted that SWIFT operates in Canada; collects personal information from and discloses it to Canadian banks as part of a commercial activity; and charges a fee to the banks for providing this service. Several of its shareholders and one of its directors were Canadian. While acknowledging that SWIFT's operations in Canada make up only a small percentage of the organisation's global business operations, the Commissioner noted that SWIFT has a significant presence in that country and was therefore subject to Canadian law.

13. In another high-profile case, a French lawyer was convicted in France of "the crime of disclosure of economic, commercial, industrial, financial or technical documents or information that are to constitute evidence for a foreign proceeding",[16] when he sent documents to the U.S. pursuant to a U.S. court discovery order without receiving the proper consent in France to do so. This action, despite being required by a U.S. court, violated French law, and the French attorney was criminally prosecuted in France as a result. The resulting sanctions case went to the French Supreme Court, which upheld the conviction and the €10,000 fine.[17] This may be the first case where a litigant has been tried in another jurisdiction for attempting to comply with a U.S. discovery order, but the example illustrates the importance of finding an appropriate balance between the requirements of effective cross-border judicial co-operation (in this case, the taking of

---

[14] Expert Group of the OECD, *Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* (23 September 1980), Paris, OECD, para. 75.
[15] *Ibid*., para. 76.
[16] The crime was a violation of article 1 bis of Law No. 68-678 of July 26, 1968, as incorporated by Law No 80-538 of July 16, 1980.
[17] *In re Advocat "Christopher X*," No. 07-83228 (Cour de Cassation Dec. 12, 2007).

evidence abroad) and data protection laws. Determining this balance calls for particularly careful co-ordination and close co-operation among States when data protection laws interact with the requirements of effective cross-border judicial co-operation.

14. The above examples are just a couple of high-profile instances where cross-border data transfers have raised serious questions of international jurisdiction, applicable law, recognition and enforcement or judicial and administrative co-operation. There are indeed quite a high number of such cases; those provided above are simply to illustrate the chilling effect on commerce and cross-border transactions the uncertain data protection regime has created in its current state.

B. Legislative reactions

15. With the rise of cases caused by conflicting data protection regimes, some legislators have attempted to delimit the (extra)territorial application of data protection regimes, where available.

16. Article 4 of the EU Data Protection Directive[18] was one of the first instruments that explicitly addressed the issue of applicable law with respect to cross-border transfers of personal data. Additionally, in its Working document "Privacy on the Internet",[19] the Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party" or "WP29"[20] identified a clear need to specify the concrete application of the rule on applicable law of the EU Data Protection Directive.[21]

17. A recent WP29 opinion,[22] however, acknowledges that under the EU Directive, it is not always clear whether EU law is applicable, which Member State law is applicable and

---

[18] Article 4 of the Directive (5/46/EC) (hereinafter "Article 4") reads as follows:

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions, which could be initiated against the controller himself.

[19] Working Party 29 Opinion 5063/00/EN WP 37, *Privacy on the Internet - An integrated EU Approach to On-line Data Protection*, WP 37 (21 Nov. 2000).

[20] WP29 is an independent advisory body on data protection and privacy in the EU.

[21] WP29 also notes the objective of Article 4 is twofold: it aims at avoiding gaps (*i.e.,* no data protection law would apply) and at avoiding multiple/double application of national laws. As the EU Data Protection Directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case (*i.e.,* the law where the controller is established or where equipment is used to process personal data), it seems to provide a "rule of conflict" and no recourse to other existing criteria of private international law is necessary. See Working Party Opinion 5035/01/EN WP 56, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites* (30 May 2002). In practice, however, the EU Data Protection Directive does not adequately resolve this issue, particularly in cases where a multi-national entity is "established" or uses equipment in multiple Member States that apply the Directive differently.

[22] Working Party 29 Opinion 02356/09/EN WP 168, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (1 December 2009). *See also* Working Party 29 Opinion 00350/09/EN WP 159, *on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)* (10 February 2009).

the applicable law(s) in case of multiple establishments of a multinational in different member States.[23]

18. For example, it is very common for the operators of websites to set "cookies" on to the browser programs of those visiting their sites. Such a mechanism operates automatically once established and arguably collects personal data from users of the site. If a website operator based in a non-European country were to place cookies on the browser programs of persons situated within the EU, then the operator's actions would arguably meet the applicable law criteria in the EU Directive found in Article 4. This would mean that the processing would be governed by the data protection law of the EU Member State concerned and could in practice extend the data protection laws of this one jurisdiction to companies worldwide simply by virtue of the fact that a person located in Europe accesses a website that uses cookies.

19. WP29 is currently drafting an opinion on the concept of applicable law and plans to advise the European Commission on this topic in the course of the upcoming year. WP29 has also called upon the European Commission to investigate the feasibility of a binding international data protection framework. In the absence of global legal standards, the Commission was asked to promote the development of data protection legislation based on the Madrid Resolution's Joint Proposal on International Standards for the Protection of Privacy.[24]

20. Similarly, in addition to attempts to address applicable law issues in Europe, the Australian Law Reform Commission (ALRC) recently issued a Report that includes a chapter on cross-border data flows.[25] This Report sets forth a principle for cross-border data flows whereby the personal data collection entity remains accountable for that personal information unless the recipient is subject to a law or other binding mechanism that effectively upholds privacy protections that are substantially similar to those in Australia, consent from the data subject is obtained, or the entity is required or authorised by law to transfer the personal information. This principle seems to be a combination of approaches taken by other regimes or collective entities.

C. Going forward?

21. Cross-border data protection issues can be addressed from a private international law angle. For example, there is indeed a need to determine how to allocate jurisdiction for protection of privacy in cross-border data flows or which data protection law applies to a particular act of data processing. Concerns about an extraterritorial application of data protection laws and its effects on the recognition and enforcement of decisions abroad have arisen.

22. It is clear from the initiatives and cases discussed above that different data protection regimes in different parts of the world represent an obstacle to economic activities that require a constant flow of information. While a number of regional instruments and other less formal arrangements exist to facilitate cross-border enforcement and co-operation, there is yet no system in place to address fundamental cross-border issues from a global private international law perspective.

---

[23] See *supra* note 22, Working Party 29 Opinion 02356/09/EN WP 168, p.9.

[24] See http://www.privacyconference2009.org/media/Publicaciones/index-iden-idweb.html (last consulted 31 March 2010).

[25] Voir http://www.austlii.edu.au/au/other/alrc/publications/reports/108/ (last consulted 31 March 2010), in particular Chapter 31.

23. There is growing awareness of the need to co-ordinate work in this area. Privacy enforcement authorities continually cite significant challenges in addressing cross-border cases. According to an OECD report, a majority of these authorities indicate that "they would benefit from improved powers to carry out investigations either jointly or at the request of another authority" and that "efforts by authorities in the cross-border context are sometimes limited by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints".[26] The same report concluded that "there is considerable scope for a more global and systematic approach to cross-border privacy enforcement and co-operation".[27]

24. In doctrinal writings, the most relevant research conducted to date is that by Christopher Kuner. Mr Kuner's most recent articles, "An International Legal Framework for Data Protection: Issues and Prospects",[28] and "Data Protection Law and International Jurisdiction on the Internet"[29] examine calls for a global legal framework for data protection, and in particular suggestions that have been made in this regard by the International Chamber of Commerce and various national data protection authorities. The articles consider the various options through which an international framework could be enacted, before drawing some conclusions about the form and scope such a framework could take, the institutions that could co-ordinate the work on it, and whether the time is ripe for a multinational convention on data protection. Interestingly, the conclusions to his last article (focusing on international jurisdiction) read as follows:

> "International bodies dealing with international jurisdictional issues (such as the Hague Conference on Private International Law, UNCITRAL, and others) have had little interest in data protection law; most scholarly articles and books dealing with jurisdiction on the Internet have devoted little space to data protection issues; and data protection regulators have shown little understanding of issues of international jurisdiction (…). Another problem is that in many cases, data protection regulators assert jurisdiction over foreign entities processing personal data without giving a clear explanation of the jurisdictional basis. If more workable rules for jurisdiction under data protection law are to be developed, then those working in the field of international jurisdiction have to devote greater attention to issues under data protection law, and data protection regulators and scholars need to have a greater understanding of the law of international jurisdiction."[30]

25. In short, multiple approaches have been taken or suggested to address cross-border data protection issues, but none have yet to successfully create a system that affords certainty and clarity to private individuals or government officials charged with oversight or enforcement.

---

[26] *Report on the Cross Border Enforcement of Privacy Laws* (18 October 2006), OECD, Paris.
[27] *Ibid.*
[28] C. Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," *Computer Law & Security Review*, Vol. 25, pp. 307-317, 2009.
[29] C. Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis", forthcoming in the *International Journal of Law and Information Technology* (Parts 1 and 2), 2010.
[30] *Ibid.*, Part 2, p. 20.

26. Another significant element is the inclusion of this topic on the agenda of the Madrid International Conference of Data Protection and Privacy Commissioners. Under the suggestive title of one of the Conference panels: "*We cannot help you. Your data are in international waters*",[31] representatives of the private sector, legal practitioners and international officials examined the difficulties encountered by global players when managing cross-border data flows in practice. A member of the Permanent Bureau contributed to the discussion by presenting to the international data protection community some of the tools that have been developed for the effective monitoring of the Hague Conference Conventions and suggested that certain models of international co-operation may be adequate for the challenges privacy enforcement authorities face.

27. The Madrid participants recognised that it was difficult to identify a set of core principles which would take into account regional differences without modifying the level of protection afforded by those regions which have a well-established data protection regime enshrined in law.

28. In addition, earlier drafts of the *Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the processing of Personal Data*[32] proposed a means for establishing the relevant jurisdiction and law applicable to cross-border data transfers. It is important to note that these provisions had to be removed from the final draft put forth at the Madrid Conference, suggesting that the development of a solution to jurisdictional and applicable law questions is not yet readily apparent.

29. Several delegations at the Madrid Conference and in subsequent consultations with the Permanent Bureau, however, expressed interest in the idea of administrative co-operation between privacy regulators and the possible model role of Hague Conference instruments in particular. The Hague Conference should therefore continue to offer its expertise based on a long tradition of dealing with legal issues where national legislation varies significantly throughout the world or simply has yet to be adopted.

IV. Conclusion

30. This is an area of law where international co-operation and co-ordination for cross-border cases may be a way forward. In this document, the Permanent Bureau has endeavored to summarise the current state of affairs with respect to cross-border data protection issues in order to highlight ways in which the Hague Conference may provide a valuable contribution in this area.

31. Based on the information provided above, the Hague Conference could and should, subject to the views of the Council, play a role in this area, in line with its mandate and limited resources. In particular, the Permanent Bureau is willing to continue to monitor recent developments, take active part in discussions and offer its assistance where appropriate, in particular with a view to:

[31] This panel was asked to discuss issues that may arise when data subjects surf the Internet (or engage in some other multi-jurisdictional transaction). For example if a consumer visits a website and it turns out that the owner of the domain is a company with headquarters in a third country, which in turn is different from that of the servers where the information is kept, most likely contracted by a third company providing hosting or housing, and also different from the country of the user that has just registered, what would be the applicable law in the event of any disputes? What international rules could be used to determine jurisdiction and applicable law? Are new specific rules to determine the applicable law? These questions simply underscore the uncertainty in this area.

[32] See *supra* note 24.

- Identifying possible uncertainties on the applicable law to cross-border data flows necessary to the application of Hague Conventions.
- Assessing the feasibility of tools already successfully implemented by the Hague Conference on transnational co-operation and co-ordination in other contexts as models for cross-border data flow questions.
- Contributing to the ongoing debate whether additional multilateral efforts are feasible and/or desirable and whether it would bring added advantages with respect to existing instruments.