BINDING CORPORATE RULES FOR CROSS-BORDER DATA TRANSFER

David Bender[1] & Larry Ponemon[2]

I. INTRODUCTION

Companies today confront unprecedented legal challenges when they seek to transfer personal data between different nations. Many nations have recently enacted "data protection" laws, designed to protect the personal information of individuals. Although protecting the personal information of individuals is surely a worthwhile goal, the enactment of these laws has nevertheless encumbered the ability of companies to process and move the personal data they collect. The legal challenges faced are perhaps greatest as they relate to multinational or global companies, many of which are based in the United States. This article describes the nature of these problems, the status of one potential solution that many companies are pursuing – "binding corporate rules" ("BCRs") – and offers the findings from Ponemon Institute's 2003 & 2005 Benchmark Study on Corporate Privacy Practices[3] on how companies are responding to global privacy standards.

A. THE CROSS-BORDER TRANSFER REQUIREMENTS OF A U.S.-BASED MULTINATIONAL

It is no secret that commerce has become increasingly international. As a result, commerce now requires the transfer of huge quantities of personal data,[4] largely relating to employees and customers. Such data transfers often occur

---

[1] David Bender, Esquire is of counsel at White & Case in New York, New York where he co-chairs the Privacy Practice Group. Mr. Bender primarily focuses his practice on matters involving privacy, intellectual property, and information technology.

[2] Dr. Ponemon is the chairman and founder of the Ponemon Institute and a partner and privacy advisor to Peppers & Rogers Group. Dr. Ponemon is noted as a pioneer in privacy risk management and the development of the responsible information management framework. Dr. Ponemon also serves as an adjunct professor of ethics and privacy for Carnegie-Mellon University and the CIO Institute.

[3] Ponemon Institute, 2003 Benchmark Survey Corporate Privacy Practices and 2005 Benchmark Survey Corporate Privacy Practices (on file with authors) [hereinafter 2003 and 2005 Benchmark Studies], discussed *infra*.

[4] In this article, we use the term "personal data" to mean any data relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity. This definition is similar to the one adopted by the EU Data Protection Directive, which is identified and discussed *infra*.

between and among units of the same corporate enterprise that are located in different countries. This need to transfer personal data is probably most obvious in the case of global corporations that conduct business in a host of nations around the world, many of which are headquartered in the United States.

Many (if not most) of these global enterprises operate centralized Human Resource ("HR") and customer databases in a single location or in a small number of regional locations. HR data and customer data gathered worldwide are then transferred from the collection point to computers in the single centralized location or the several regional locations. In most of these companies, this manner of data collection and transfer was established long ago, and the computer and the telecommunications systems that support the transfers are quite sophisticated. Accordingly, for the typical global enterprise today, cross-border transfer of personal data is both critical and complex.

B. THE NATURE OF DATA PROTECTION LAWS

During the past decade or so there has been a proliferation of a type of privacy law known as a "data protection" law. Data protection laws require government and commerce to adhere to certain basic privacy requirements in their "processing"[5] of personal data.[6] The rationale generally given for such laws is that they protect fundamental human rights, possessed by every individual, in the personal data related to him or her.[7] Many of the strictest data protection limitations present themselves in the laws adopted by European Union ("EU") member states pursuant to a requirement in the EU Data Protection Directive[8] (hereinafter, the "Directive") to enact such laws. This article focuses primarily on the EU member state data protection laws promulgated pursuant to the Directive.

---

[5] The term "processing" is broadly defined to include any operation that is performed on the data, and includes: storage, consultation, transmission, retrieval, adaptation, and a host of other operations. EU Data Protection Directive 95/46, Art. 2, 1995 O.J. (L 281) 31 (EC) [hereinafter EU Directive].

[6] These laws generally relate to data quality and to data processing. Examples of laws relating to data quality include laws that require fair and lawful processing; collection only for specified purposes; collection only of sufficient data to satisfy the purposes of the collection; maintenance of accuracy (including updating) in the data; and destruction when the data is no longer needed for the purpose for which it was collected. *See, e.g.*, EU Directive, *supra* note 5, at Art. 6, pts. 1(c)-(d). Examples of laws that relate to data processing include requirements that "data subjects" (*i.e.*, the individuals to whom the data pertains) give consent; or that the processing be necessary for one of a number of enumerated purposes. *See, e.g.*, EU Directive, *supra* note 5, at Art. 6, pts. 1(a)-(b).

[7] *See, e.g.*, EU Directive, *supra* note 5, at Pmbl.

[8] EU Directive, *supra* note 5. In the EU a "directive" is a decree promulgated by the EU and requiring each of the twenty-five member states to enact national legislation implementing the minimum requirements set forth in the directive. Treaty on European Union (Maastricht Treaty), Feb. 7, 1992, 1992 O.J. (C 191) 1 *amended at* 2002 OJ (C 325) 5.

C. DATA PROTECTION LAWS AS APPLIED TO CROSS-BORDER TRANSFER

Although some nations with data protection laws have no restrictions on cross-border transfer, many others do.[9] Pursuant to the Directive, transfer from an EU member state to a nation outside the EU is permitted only where (i) the transferee nation has "adequate" data protection laws by reason of its domestic laws or international commitments; (ii) the data subject has given unambiguous consent; (iii) the transfer is necessary for the performance of a contract between the data subject and the controller of the data, or for one of several other specific purposes; (iv) the transfer involves data that is essentially public; or (v) there is in place between data exporter and importer a contract that, in the view of the pertinent member state or the EU, requires adequate safeguards by the importer.[10]

II. DISSATISFACTION WITH THE TRADITIONAL METHODS OF ACHIEVING CROSS-BORDER COMPLIANCE

A. "ADEQUATE" LAWS

The EU Directive establishes a relatively high standard for data protection, and the EU generally has been unwilling to settle for much less than that standard in its consideration of whether other nations have "adequate" data protection laws. Among major nations, only Argentina, Canada (for certain purposes), and Switzerland have been deemed by the EU to have adequate data protection laws.[11] The domestic data protection laws of the United States, which are sector-specific and have no general applicability, have been deemed by the EU not to be adequate.[12] However, in 2000 the EU and the U.S. Department of Commerce ("DOC") reached an agreement regarding the "Safe Harbor Principles" that permits export from the EU to the United States under certain conditions.[13]

---

[9] *Compare* United States (no restrictions), *with* Argentina, Canada, Switzerland, Isle of Man, Bailiwick of Guernsey (restrictions).

[10] EU Directive, *supra* note 5, at Arts. 25, 26.

[11] Commission Decision 2000/519/EC, 2000 O.J. (L 215) 4-6 (EC). Hungary was also deemed by the EU to have adequate data protection laws, but subsequently (on May 1, 2004) became an EU member state.

[12] Article 29 Data Protection Working Party, *Working Paper: Level of Data Protection in the United States and Ongoing Discussions Between the European Commission and the United States Government*, DG MARKT 5093/98, WP15 (Jan. 26, 1999) (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/1999_en.htm (last visited Mar. 22, 2006)).

[13] Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7-47 (EC).

There is general dissatisfaction among multinationals with the compliance method of adequate laws. These companies complain that the standard is too high because the laws deemed "adequate" by the EU impose too heavy a burden on the company without a commensurate increase in benefit to the data subject.

1. THE SAFE HARBOR PRINCIPLES

When a company in the United States notifies the DOC that it has certified to the Safe Harbor Principles, the company's name is posted on the DOC's Safe Harbor Web site in confirmation of its certification.[14] By so certifying, a company represents that it has adopted a privacy policy that complies with the Safe Harbor Principles. Any company doing business in the United States that is subject to the jurisdiction of the Federal Trade Commission (the "FTC") or the Department of Transportation is eligible to certify.[15] The number of companies certifying is thus far less than predicted; as of this writing, some 848 companies have certified.[16]

There are seven Safe Harbor Principles: Notice, Choice, Access, Security, Enforcement, Onward Transfer, and Data Integrity.[17] "Notice" refers to the requirement that the company inform data subjects about the purposes of its data collection and use, the types of disclosees, and the options for limiting use and disclosure.[18] "Choice" refers to the requirement that data subjects be offered the opportunity to determine whether and how their data will be used and disclosed.[19] "Access" is directed to the requirement that data subjects be able to gain access to their data so as to correct or direct the deletion of inaccurate data.[20] "Security" relates to the requirement that the company take reasonable steps to protect the data from loss, misuse, unauthorized access, alteration and destruction.[21]

---

[14] U.S. Department of Commerce, Safe Harbor, http://www.export.gov/safeharbor/ (last visited Mar. 7, 2006) [hereinafter Safe Harbor].

[15] Thus, companies in certain important sectors of the economy (*e.g.*, telecommunications and financial services) are not eligible to certify because they are governed by neither the FTC nor the Department of Transportation.

[16] Safe Harbor, *supra* note 14.

[17] http://www.export.gov/safeharbor/sh_overview.html (last visited Mar. 22, 2006).

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

"Enforcement" concerns the requirement that the company provide to the data subject some affordable, readily available mechanism for assuring compliance with the Safe Harbor Principles.[22] "Onward Transfer" is directed to the requirement that once in the United States, the data will only be disclosed to third parties, consistent with the principles of notice and choice, or pursuant to an agreement imposing on the disclosee a level of protection at least as high as that required by the Safe Harbor Principles.[23] "Data Integrity" refers to the requirement that the data be processed only in conformity with the purposes for which it was collected, and that reasonable steps be taken to maintain its reliability for its intended use.[24]

The biggest problem with the Safe Harbor Principles is probably that they are not sufficiently universal because they apply only to transfer from the EU to the United States. Accordingly, these provisions apply neither to transfers from a non-EU nation to the United States, nor to transfers from the EU to a nation other than the United States. Also, some companies have voiced dissatisfaction over the need to re-certify (and have another privacy audit conducted) annually.[25] And, for a time, the EU seemed displeased that no complaints were made to any of the EU member state data protection authorities ("DPAs")[26] or to the FTC; this was viewed by the EU as evidence that the Safe Harbor system was not working.[27] However, by the end of 2005, the EU had reversed its position and began singing the virtues of Safe Harbor, suggesting that for the transfer of data from the EU to the United States, it provided the optimum vehicle.

B. CONSENT

There are a number of bases for dissatisfaction with the vehicle of consent. First, several EU member states have taken positions questioning an employee's ability to give the type of unambiguous consent that is necessary here, suggesting

---

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *See* http://www.export.gov/safeharbor/sh_registration.html (last visited Mar. 22, 2006).

[26] The Directive required each member state to create a government agency responsible for implementing and enforcing its national law enacted pursuant to the EU Directive. EU Directive, *supra* note 5, at Art. 28. These agencies are known generically as DPAs. *Id.*

[27] Commission Staff Working Document, *SEC on 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 U.S. Department of Commerce* (Oct. 20, 2004) (available at http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm (last visited Mar. 22, 2006)).

that the consent vehicle is not available with regard to employee data.[28] With some other types of personal data, an issue arises of what to do with regard to the data about individuals who do not provide the requested consent. In some instances this data can be segregated into a separate database, but in other situations, it will not be feasible to segregate this data. Thus, the lack of universal consent will render consent unusable as a basis for effecting a legal transfer. Moreover, even where segregation is possible, it will often be rather cumbersome and may result in additional expenses.

C. "NECESSITY"

The problem with using necessity as a basis for transfer is the narrow interpretation given to the term by most of the DPAs. As the following example illustrates, if a U.K. resident makes a reservation in London with a U.S.-based airline, the airline may transfer the reservation data (some of which may be personal data) to its main reservations computer in the United States. Such transfers have been challenged as not being in compliance with the data protection laws.[29] The airline argues that the transfer to the United States is proper as "necessary" to its performance of a contract with the data subject. But typically the DPA's position is that although transfer to a reservations computer is necessary, it is not necessary that the computer receiving the data transfer be located outside of the EU. Global corporations generally view this as a very narrow interpretation of "necessity," which drastically limits the usefulness of this vehicle.

---

[28] Article 29 Data Protection Working Party, *Working Paper*: *Processing of personal data in the employment context*, DG MARKT 5062/01, WP48 (Sep. 13, 2001) [hereinafter WP 48] (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm (last visited Mar. 22, 2006)); Article 29 Data Protection Working Party, *Working Paper*: *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP114 (Nov. 25, 2005) (citing WP 48) (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm (last visited Mar. 22, 2006); Blas, Diana Alonso, Senior International Officer, Dutch Data Protection Authority, *Policy paper on transfers of personal data to third countries in the framework of the Dutch Data Protection Act (WBP)*, p. 18 (Feb. 2003) (citing WP 48) (available at http://www.dutchdpa.nl/downloads_int/nota_derde_landen_en.pdf?refer= true& theme=purple (last visited Mar. 22, 2006)); Hellenic Data Protection Authority: *Directive No. 115/2001*, Section C, para. 4 (Sep. 20, 2001) ("regarding the case of employment relations, the innate inequality of the parties and the generally applying dependency relationship of the workers creates doubts concerning the freedom of workers' consent, a necessary element for the validity of processing") (available at http://www.dpa.gr/decision_eng.htm (last visited Mar. 22, 2006)).

[29] *See e.g.*, *American Airlines Challenges Swedish Data Protection Board's Authority*, (Nov. 13, 1998) (available at http://www.privacyexchange.org/news/archives/nf/ newsflash981116.html (last visited Mar. 22, 2006)).

D. STANDARD CONTRACTUAL CLAUSES

Transfer under a contract, executed by data exporter and data importer, that has been approved by the EU or the appropriate DPA, renders a transfer proper. Effective September 3, 2001, the EU adopted a set of standard contractual clauses ("SCCs")[30] for transfer from an EU exporter to a non-EU data "controller."[31] Thereafter, effective April 3, 2002, the EU adopted a set of SCCs for use in connection with a transfer to data "processors."[32] Both of these sets of SCCs were criticized by U.S. companies on several bases. First, they grant third party beneficiary rights to data subjects, with a right to enforce the agreement.[33] Second, these SCCs choose the governing law to be that of the EU exporting member state.[34] In addition, they require the importer to submit to dispute resolution in that member state.[35] A copy of the agreement must be deposited with the DPA of the exporter if the DPA so requests,[36] and that DPA has a right to audit the agreement.[37] Finally, they provide for joint and several liability between exporter and importer.[38]

Because of its dissatisfaction with these two sets of SCCs, the business community, through trade organizations such as the International Chamber of Commerce, drafted its own less onerous proposed SCCs, and sought EU approval for them.[39] Effective April 1, 2005, the EU approved a set of controller SCCs submitted by the business community as an alternative to the original controller

---

[30] Commission Decision 2001/497/EC, 2001 O.J. (L 181) 19-31 (EC).

[31] A "controller" is a natural or legal person that determines the means and purposes of processing personal data. *See* EU Directive, *supra* note 5, at Art. 2, pt. 1(d).

[32] A "processor" is a natural or legal person that processes personal data on behalf of its controller. *Id*. at Art. 2 pt. 1(e).

[33] Commission Decision 2002/16/EC, 2002 O.J. (L 6) 52-62 (EC).

[34] *Id*. at 54

[35] *Id*.

[36] *Id*.

[37] *Id*. at 53.

[38] *Id*. The two parties are, however, permitted to enter into an indemnity agreement. *Id*. at 53.

[39] Article 29 Data Protection Working Party, *Working Paper*: Draft standard contractual clauses submitted by a group of business associations ("the alternative model contract"), MARKT/11754/03/EN, WP84 (Dec. 17, 2003) (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm (last visited Mar. 22, 2006)).

SCCs.[40] Under these alternative SCCs, while still a third party beneficiary, the data subject can enforce those rights only after the exporter has failed to act for a period of 30 days.[41] Also, there is no joint and several liability of the parties, but the exporter has a due diligence obligation to determine that the importer can perform its obligations under the SCCs.[42] Also, the audit provision is less stringent than in the original SCCs. While many companies who have considered the matter prefer the alternative controller SCCs, many of the criticisms regarding the original controller SCCs still apply.

III. THE NATURE OF BCRS

At this time the term "BCRs" is still only loosely defined, and relates more to a concept than a distinct and clearly articulated vehicle.[43] Nevertheless, the concept has attracted much attention, especially among global corporations. Their interest in BCRs is twofold: to diminish the amount of paper and effort attendant to legitimizing their transfers,[44] and to impose less stringent requirements on their transfer activities. At this time, one can count using the fingers on one hand the sets of BCRs that have actually been approved.[45] Most of those have been approved by only a single state.[46]

The concept of BCRs is simply this: A code of conduct setting forth the privacy policy of the entire enterprise is drafted, to which each entity included in the enterprise subscribes, enabling data subjects and other entities to enforce that code against the entity/enterprise.[47] Many global enterprises believe that codes of conduct should be sufficient for the cross-border transfer of personal

---

[40] Commission Decision 2004/915/EC, 2004 O.J. (L 385) 74-84 (EC).

[41] *Id*. at 75.

[42] *Id*. at 74.

[43] Article 29 Data Protection Working Party, *Working Paper: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, MARKT/11639/02/EN, WP74 (June 3, 2003) [hereinafter WP 74] (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm (last visited Mar. 22, 2006)).

[44] For example, if an enterprise with a dozen exporting units in the EU and thirty importing units outside the EU were to use SCCs, it might require some 360 separate sets of SCCs.

[45] *See, e.g.*, Robert Bond, *Data Transfers: First U.K. Authorization of Binding Corporate Rules*, BNA Int'l, http://newsweaver.co.uk/eletra.html.

[46] *Id.*

[47] WP 74, *supra* note 43.

data.[48] The two problems that present themselves with respect to any specific set of BCRs deal with the specific terms that the code would be required to include, and the enforceability of the BCRs. On the first point, one major issue is whether the BCRs must include terms similar to those in one of the sets of SCCs, or whether some or all of the provisions that have triggered criticism may be eliminated or ameliorated. On the second point (which implicates national law and might be answered differently in different nations), one issue is whether BCRs would bind an enterprise when, for example, one of its entities exports to itself.[49]

IV. ADVANTAGES AND DISADVANTAGES OF BCRS FOR A U.S.-BASED MULTINATIONAL

It is difficult to discuss the details of BCRs because they are still largely a developing concept, albeit an important one. Nevertheless, the following comments are offered.

A. ADVANTAGES OF BCRS

BCRs offer the possibility of imposing a more flexible privacy regime than any of the other available methods of transferring data across borders. The enterprise itself writes the code of conduct, and can therefore fashion it to reflect its own needs.[50] One imponderable at this point is how far from the SCCs one can wander, and still obtain approval. Accordingly, there is a potentially major advantage here, but we won't know for whether it is genuine until BCRs become more widely used.

B. DISADVANTAGES OF BCRS

A major disadvantage attendant to BCRs is the uncertainty that pervades their use. An enterprise that needs a rapid solution to its cross-border needs must either take the validity of the BCR approach on faith and plunge ahead with it – a rather perilous course – or must look to some other vehicle for legitimizing its cross-border transfers. Another disadvantage for global enterprises is the reduction in efficiency that arises from substituting possibly hundreds of other documents for a single document.

---

[48] *See, e.g.*, Bond, *supra* note 45 (referring to General Electric).

[49] For example, if IBM Corp., a New York corporation, receives a data transfer from a subsidiary located in a European Economic Association ("EEA") nation.

[50] *See* WP 74, *supra* note 43, at p. 8.

V. THE EU'S PRESENT POSITION ON BCRS

The EU's receptivity to BCRs has increased significantly in the past year, and presently – in its official publications – it purports to favor legitimizing this vehicle.[51] But in practice, for a number of reasons, it may still prove difficult to use BCRs for transfer from more than a single EU member state. The EU position is set forth in three documents released by an EU organ known as the Article 29 Working Party.[52] The three documents are: WP 74,[53] WP 107,[54] and WP 108.[55]

In WP 74 the Working Party states that BCRs would be a viable alternative for cross-border transfer, but suggests a regime that many multinationals view as so burdensome that their main incentive (limiting the burden and expense of compliance) would not be met. In this document the Working Party seems to take the view that BCRs must meet the same requirements as SCCs.[56] Also, as a procedural matter, the Working Party notes that BCRs must be approved by the DPA in each exporting member state, although it suggests that one DPA take the lead.[57]

WP 107 and WP 108 significantly clarify much of what was set out in WP 74. WP 107 sets forth a general procedure under which a corporate enterprise interested in using BCRs for export from more than one EU Member State may seek to do so.[58] The DPAs are not required to accept or approve BCRs so

---

[51] *See id*., at p. 21.

[52] The Article 29 Working Party is an independent EU Advisory Body on Data Protection and Privacy, so named because it owes its existence to Article 29 of the Directive. EU Directive, *supra* note 5. Its tasks are set forth in Article 30 of the Directive, *id*. at Article 30, and amplified in Article 14 of a subsequent directive. Council Directive 97/66 Article 14, 1998 O.J. (L 24) 1 (EC).

[53] WP 74, *supra* note 43.

[54] Article 29 Data Protection Working Party, *Working Paper*: Co-Operation Procedure for Issuing Common Opinions as Adequate Safeguards Resulting From "Binding Corporate Rules" WP107 (Apr. 14, 2005) [hereinafter WP 107] (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm (last visited Mar. 22, 2006)).

[55] Article 29 Data Protection Working Party, *Working Paper*: Establishing a Model Checklist Application for Approval of Binding Corporate Rules, WP108 (April 14, 2005) [hereinafter WP 108] (available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm (last visited Mar. 22, 2006)).

[56] WP 74, *supra* note 43, at pp. 5-6.

[57] *Id*. at p. 11.

[58] WP 107, *supra* note 54, at p. 2.

prepared.[59] The initial step is to select a lead DPA.[60] The selection should be based on five criteria,[61] the most important of which is the location of the enterprise's European headquarters.[62]

The DPA receiving the application must exercise discretion in deciding whether, under these criteria, it has been appropriately designated as the DPA.[63] If not, it may select a different DPA.[64] That DPA which receives the application should be provided with appropriate information intended to justify the proposal, including the nature and general structure, the means and purposes of processing in the EU/EEA (especially the locations of the decisions, the location and nature of EU affiliates, the number of persons concerned, the places from which export from the EU takes place, and the identity of the importing nations.[65] The receiving DPA then forwards information regarding selection of the lead DPA to DPAs in all the other exporting Member States, with an indication of whether it agrees to be the lead DPA.[66] If it agrees, other DPAs will have two weeks to object.[67] If the receiving DPA does not agree to be the lead, it should give its reasons and recommend a lead DPA, in which case the affected DPAs shall endeavor to decide the matter within one month.[68]

---

[59] *Id.*

[60] *Id.*

[61] *Id.* The five criteria are (i) the location of the enterprise's European headquarters; (ii) the location of the particular unit responsible for data protection; (iii) the location of the particular unit best situated to deal with the application and enforce the BCRs; (iv) the location where most decisions regarding the purposes and means of processing are made; and (v) the Member States from which most transfers to locations outside the European Economic Association ("EEA") will take place. The EEA comprises the 25 EU member states, plus Iceland, Liechtenstein, and Norway. EEA Enlargement Agreement, 2004 O.J. (L 130) 3 (EC).

[62] As specified in WP 74, if the enterprise's headquarters is not in the EU, it should delegate data protection responsibility to an EU member. *Supra* note 43, at p. 11. In particular, that member should be responsible for ensuring that the processing of any foreign member complies with the BCRs, for interfacing with the lead DPA, and for paying compensation for damages resulting from violation by any member of the enterprise of the BCRs. *Id.*

[63] WP 107, *supra* note 54, at p. 2.

[64] *Id.*

[65] *Id.* at p. 3.

[66] *Id.*

[67] *Id.*

[68] *Id.*

The lead DPA and the applicant will circulate a "consolidated draft" to all the concerned DPAs, who may comment within one month.[69] Comments will be transmitted to the applicant, which will discuss them with the lead DPA.[70] If the lead DPA believes the applicant can address all comments satisfactorily, it will invite a "final draft," and will invite the other DPAs to confirm that draft.[71] If the other DPAs do confirm, that will be deemed as an agreement to permit the BCRs, although additional requirements may still exist in each nation, such as notification or administrative formalities.[72] The Chair of the Article 29 Working Party will be informed of the decision and will inform the other DPAs.[73] First and consolidated drafts should be provided in the language of the leading DPA and English.[74] The final draft should be translated into the language(s) of all concerned DPAs.[75]

WP 108 is largely a checklist for seeking approval of BCRs.[76] WP 108 "concentrates on the matters that a DPA needs to consider in the assessment of adequacy," and explains that participation of any DPA in the BCR approval process is voluntary and can be made on a case-by-case basis.[77]

WP 108 deals with the information that must be supplied.[78] The document must include contact information for the responsible person, information sufficient to justify choice of the lead DPA, and all documents comprising the BCRs.[79] The application should also indicate how the rules in the BCRs will be legally binding within the enterprise, and how they will provide for the benefit of data subjects.[80] WP 108 sets forth a few suggestions as to how BCRs may be binding on the companies comprising the enterprise: a set of

---

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.* at p. 4.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] WP 108, *supra* note 55. As indicated by its title, WP 108 is a checklist.

[77] *Id.* at p. 2.

[78] *Id.* at pp. 3-4.

[79] *Id.*

[80] *Id.* at pp. 5-7.

contractual rules; unilateral declarations or undertakings by the parent and binding on the other members; regulatory measures such as contained in statutes; or other rules within the general business principles of an organization, backed by appropriate policies, audits and sanctions.[81] BCRs must also bind employees, and the application must describe how employees are bound.[82] One example is a provision in the contract of employment, with disciplinary procedures.[83] Adequate training and senior staff commitment are also necessary.[84] The BCRs must also bind any subcontractors, and the application should set out clauses that will be used for this purpose in subcontractor agreements, as well as explain how the contracts will deal with non-compliance.[85]

Finally, data subjects must be able to enforce compliance with the BCRs through both DPAs and courts.[86] A data subject must be able to commence a claim, at his or her option, in the nation from which the export took place, or in the nation of the enterprise's EU headquarters (or the nation of the EU enterprise member that has data protection responsibility).[87] The application should delineate the actual steps a data subject should take to obtain a remedy, and should confirm that the EU headquarters (or the responsible EU company) has assets (or arrangements) sufficient to satisfy a claim for damages caused by any part of the enterprise.[88] The application should also identify the entity that will handle claims, describe access to the claim-handling process, and note that the burden of proof regarding breach of BCRs will fall on the enterprise.[89] In addition, the application should acknowledge that data subjects will have the rights specified under the EU Data Protection Directive,[90] and should agree to cooperate with DPAs and abide by their advice.[91]

---

[81] WP 108 notes that local advice is required in determining what may or may not be binding. *Id.* at p. 5.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.* at p. 6.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] EU Directive, *supra* note 5.

[91] WP 108, *supra* note 55, at pp. 6-7.

WP 108 deals also with verification of compliance.[92] The BCRs must provide for an audit, and the audit program/plan should be clearly set out in a document that shall be provided to a DPA on request.[93] The auditors may be external, internal, or both. The enterprise should also summarize its audit arrangements and the manner of internal handling of audit reports.[94] Further, the BCRs should identify the nature of the data to be transferred (e.g., human resources) with sufficient detail for a DPA to determine whether adequate safeguards against unauthorized use, disclosure, etc., are in place.[95] The BCRs should also describe the purposes for which the data are processed, and the scope of transfers that are covered by the BCRs,[96] whether they cover intra-EU transfers, and the basis for onward transfer from importers to third parties.[97]

The BCRs should also describe safeguards required by the Directive and how they are met in the enterprise.[98] In particular, they should address transparency and fairness to data subjects; purpose limitations; ensuring data quality; security; data subject access/correction rights; and restrictions on onward transfer.[99] Finally, the BCRs must have in place a system for informing all companies comprising the enterprise, as well as pertinent DPAs, about changes to the BCRs.[100]

VI. BENCHMARK STUDY ON GLOBAL CORPORATE PRIVACY PRACTICES

---

[92] *Id.* at p. 7.

[93] *Id.* The DPAs are not interested in seeing proprietary information except to the extent it affects data protection compliance.

[94] *Id.*

[95] *Id.*

[96] *E.g.*, the identity of EU exporters and non-EU importers.

[97] WP 108, *supra* note 55, at pp. 7-8.

[98] *Id.* at p. 8.

[99] *Id.*

[100] *Id.* at p. 9.

The mission of Ponemon Institute is to advance responsible information management (RIM) practices in the public and private sectors.[101] Specifically, organizations should not only be in compliance with laws, but should also understand how to ensure that their business practices are in alignment with the privacy preferences of its key stakeholders. RIM is a holistic management process that establishes the roadmap for creating a privacy program that enables companies to achieve the dual benefits of creating trust and achieving compliance.

In 2003 and 2005, Ponemon Institute conducted a Benchmark Study of Corporate Privacy Practices Report to determine how organizations are creating privacy programs that mitigate risk while building trust with their key stakeholders.[102] The research conducted by the Ponemon Institute seeks answers to four basic questions:

1. What are leading companies doing today to ensure adequate compliance with the plethora of global privacy and data protection regulations?;

2. Is there a common set of business practices leading companies have adopted to ensure reasonable protection and controls over information about people and their households?;

3. Are there apparent gaps in privacy and data protection activities that create vulnerabilities for companies?; and

4. Do corporate privacy and data protection practices vary across industry sectors?

Both the 2003 and 2005 benchmark studies addressed how multinational companies are responding to global standards for privacy and data protection.[103] Both studies also focused on seven other key areas that are considered to encompass the full range of activities in a company's privacy and data protection program.[104] These areas include: Privacy Policy, Communications & Training, Privacy Management, Data Security Methods, Privacy Compliance, Choice & Consent, and Redress.[105]

---

[101] http://www.ponemon.org (last visited Mar. 22, 2007).

[102] *See* 2003 and 2005 Benchmark Studies, *supra* note 3.

[103] *Id.*

[104] *Id.*

[105] *Id.*

The two benchmark studies provide information regarding companies' actions with respect to their privacy initiatives and those actions being taken to move companies beyond compliance.[106] Survey results suggest that many global companies which responded to questions about global standards are not paying much attention to various data flows from European Union countries to their companies in the U.S. and other locations.[107] Table 1 below reports the results of survey items regarding global standards.

According to survey results, fifty-two percent of companies evaluate trans-border data flows.[108] Consequently, over forty-eight percent may be at risk for possible regulatory action, penalties, fines and possible transfer restrictions or interruptions.[109]

	Table 1: Benchmarks for Global Standards	2003 Q%	2003 Pos%	2005 Q%	2005 Pos%	Diff
1	Does your company evaluate compliance with global regulations and standards?	78%	53%	100%	54%	1%
2	Does your company attempt to comply with the European Union Safe Harbor agreement?	95%	10%	76%	10%	0%
3	Does your company attempt to comply with new Canadian privacy regulations (PIPEDA)?	67%	14%	79%	15%	1%
4	Are your privacy policies written in multiple languages when appropriate?	85%	47%	85%	48%	1%
5	Are trans-border data flows evaluated for compliance with national privacy laws?	91%	44%	85%	52%	8%
6	Does your company attempt to comply	95%	60%	100%	68%	8%

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

	with global privacy and data protection standards?					
7	Are national privacy practices, laws and regulations monitored by your company?	98%	43%	93%	56%	13%
		87%	39%	88%	43%	4%

The differences between the results generated in the 2005 and 2003 studies suggest that many respondents are spending more effort managing compliance in localities where the company operates (increase of thirteen percent).[110] Also, it appears that more companies are tackling global compliance issues as part of their overall program (increase of eight percent).[111]

The Safe Harbor Agreement offers advantages but also additional burdens for companies with overseas operations. Over ninety percent of companies surveyed have not signed on to the Safe Harbor Agreement.[112]

Survey respondents also indicate that many companies are not considering new Canadian privacy regulations (eighty-five percent), and only forty-eight percent attempt to translate privacy policies into the native languages of the targeted reader.[113]

Will BCR encourage more companies to leave the sidelines in order to comply with trans-border data flow laws? Based on Ponemon Institute's benchmark studies of corporate privacy practices, many companies are still in the early stages of implementing a privacy program to help manage their domestic compliance issues.[114] The thought of implementing a global privacy program is daunting. However, as more companies receive approval for their BCRs, the appeal of having a single, overarching compliance plan for multinational organizations will grow.

---

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*

VII. CONCLUSION

Aside from the many other significant but not critical issues remaining open, multinationals are left with two huge uncertainties: Just what will be required by way of content in BCRs, and will the DPAs in fact work together in a coordinated way to achieve the desired result?[115]

To date only a few enterprises have vigorously pursued approval for BCRs.[116] Whether this potentially useful vehicle becomes viable will depend upon whether, over the next few years, enterprises are able to (i) secure approval for sets of BCRs that contain no unduly burdensome content, and (ii) use a process in which the pertinent DPAs cooperate with each other and with the applicant. Absent success on both of these fronts, BCRs will fail and multinationals will have to consider looking elsewhere for their transfer vehicles.

[115] This is in contrast to the situation where each DPA injects its own bells and whistles into the process, thereby making it so cumbersome, expensive, and time- and effort-consuming that BCRs offer no benefit.

[116] *See, e.g.*, Bond, *supra* note 45. Daimler-Chrysler, Phillips, Shell, and General Electric have reportedly had some measure of success in this regard, but so far as the authors know, none of them have had their BCRs approved by more than a few of the desired jurisdictions.