Why are more companies joining the U.S. - EU Safe Harbor privacy framework?

By Brian Hengesbaugh, Michael Mensik, and Amy de La Lama of Baker & McKenzie LLP

This story originated as a Baker & McKenzie LLP North America Global Privacy Client Alert and is republished here with permission.

The U.S. Department of Commerce (U.S. DOC) recently held its 2009 International Conference on Cross Border Data Flows & Privacy in Washington, DC. The U.S. DOC announced at the conference that an increasing number of companies are choosing to self-certify compliance with the U.S.-EU Safe Harbor Privacy Framework (Safe Harbor). Every month, approximately 50 companies file initial self-certifications to the Safe Harbor, and approximately 150 companies submit annual re-certifications. More than 50 percent of the companies in the Safe Harbor have joined during the past two years. At present, there are more than 2,100 companies included on the U.S. DOC’s Safe Harbor list. Placed in context, this means that more companies join Safe Harbor in a single month than the total number of companies that have obtained approval for binding corporate rules to date (as discussed later, such binding corporate rules are another key approach to cross-border data transfers).

See, U.S. - EU Safe Harbor, page 4

AICPA and CICA update Generally Accepted Privacy Principles

By Nancy A. Cohen, CPA, CITP, CIPP, and Nicholas F. Cheung, CA, CIPP/C

Establishing an annual privacy risk assessment process to identify new or changed risks to personal information is a key enhancement to Generally Accepted Privacy Principles (GAPP). GAPP is an internationally recognized privacy framework developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

“An annual risk assessment is critical to understanding the privacy risks within an organization,” said Everett C. Johnson, CPA, chair of the AICPA/CICA Privacy Task Force and a past international president of ISACA. “Once those risks are identified and assessed, the organization can then take the

See, GAPP update, page 10

This Month

The year ahead: privacy predictions 2010…………………….. 3
Managing global data privacy……………………… 14
Privacy and pandemic planning………………… 15
The Lisbon Treaty and data protection………. 17
New international privacy principles for law enforcement and security………………… 18
FTC privacy roundtable signals policy shift………………………….. 20
Global Privacy Dispatches………………………… 26
Calendar of events…………………………… 29
Privacy news…………………………………… 29
Surveilled…………………………………… 30
10 privacy resolutions………………………… 34
Why are increasing numbers of companies joining the Safe Harbor? What factors cause companies to choose Safe Harbor over other approaches to addressing cross-border data transfer restrictions? This article explores some of the drivers for an increasing number of “Safe Harborites,” and identifies key differences between Safe Harbor and the alternative approaches. It also discusses special issues related to outsourcing service providers, recent enforcement actions, and trends related to global privacy compliance.

1. What is the Safe Harbor and how does it work?

The Safe Harbor is one approach U.S. companies can adopt to address the cross-border data transfer restrictions under the European Commission’s 1995 Data Protection Directive (95/46/EC) (Directive). Specifically, the Directive prohibits the transfer of personally identifiable information about individuals located in the European Union (EU Personal Data) to the United States or other locations outside the European Economic Area, unless the data recipient is subject to a law or other binding scheme that provides “adequate protection” for such EU Personal Data (Data Transfer Restriction), or otherwise qualifies for an exception to this requirement.

Examples of where the Data Transfer Restriction might apply include situations where a U.S.-based multinational needs to receive EU Personal Data relating to:

i) Employees or contractors of its subsidiaries in the EU (e.g., talent management and performance data, benefits and payroll information, data related to codes of conduct or whistleblower hotlines, or other information);

ii) Consumers or corporate customer contacts in the EU (e.g., customer relationship management or CRM data, or the like);

iii) Customers’ customers or other end users in the EU (e.g., where the multinational is an outsourcing service provider); and

iv) Other categories of individuals (e.g., job candidates, clinical trial subjects, business partners, or others).

As mentioned above, the European Commission has issued a decision that, if a U.S. organization self-certifies compliance to the Safe Harbor, it will be deemed to provide “adequate protection” and satisfy the Data Transfer Restriction for the duration of its participation in the Safe Harbor. In practice, an eligible organization in the U.S. can join the Safe Harbor by (i) conducting due diligence and taking the necessary steps to conform its data handling practices to the Safe Harbor rules (e.g., providing data subjects in the EU with a sufficient privacy notice, maintaining reasonable security for covered EU Personal Data, providing individuals in the EU with access to their own EU Personal Data, and taking other steps); and (ii) completing the self-certification form with the U.S. DOC. Once the organization completes the self-certification, its name and Safe Harbor registration will be published on the U.S. DOC’s list of Safe Harbor companies, and will be deemed to provide “adequate protection” for categories of EU Personal Data covered by its self-certification. After that point, any violation of the Safe Harbor rules can be subject to an enforcement action by the U.S. Federal Trade Commission.

2. What alternative approaches could U.S. companies use to address the data transfer restriction?

U.S. companies could also address the Data Transfer Restriction through other means, such as: obtaining express consent from the individuals at issue (Express Consent); adopting and obtaining approvals from data protection authorities for a set of binding corporate rules (BCRs); or establishing privacy agreements that conform to standard contractual clauses issued by the European Commission (Model Contracts). A brief summary of each of these options is set out here:

i) Express Consent. Five or 10 years ago, many companies adopted the Express Consent approach to international data transfers, particularly with respect to EU Personal Data about employees. Today, relatively few companies are selecting Express Consent as a comprehensive solution to addressing Data Transfer Restrictions. This is due to several factors, including concerns about “drop out” rates where some individuals may not consent, and recent opinions of data protection authorities that such consents, particularly by employees, may not be “freely given” and therefore may be invalid. It is worthwhile to note that Express Consent is still a useful solution for limited or specific situations (e.g., e-commerce offerings with “accept” clicks, employee stock options, and the like).

ii) Binding Corporate Rules (BCRs). BCRs have received significant trade press attention lately. The concept of BCRs is attractive because a group of affiliated companies will have the flexibility to develop its own articulation of privacy rules for intra-group data flows. This allows the group to tailor the rules to its actual data flows and business culture. However, the group is not free to develop whatever rules it likes—it must still comply with guidance issued by European data protection authorities regarding the data privacy principles when developing such rules. The group must also seek substantive approvals for the BCRs from the data protection authorities in the relevant EU countries. Also, BCRs only cover intra-group data transfers, and do not cover transfers to or from unaffiliated parties (e.g., service providers, business partners, M&A parties), and in practice many companies have applied BCRs to human resources data only, due in part to the complexity of obtaining approvals for customer or other categories of data. Despite recent efforts by the European data protection authorities to streamline the approval
process, the negotiations with data protection authorities for the approval for BCRs still require time and resources and tend to discourage companies from pursuing this approach unless they have significant resources to devote to the process. There are no published statistics available as to how many companies have obtained approvals for BCRs, although latest estimates indicate that the number is less than 30.

iii) Model Contracts. Model Contracts have advantages in that, unlike BCRs, the terms are pre-approved by the European Commission (no substantive data protection authority approvals required). Also, unlike Express Consent, there is no need to obtain approval from affected individuals. Although Safe Harbor shares both of these advantages, Model Contracts do have certain advantages relative to Safe Harbor, including that they facilitate cross-border data transfers from the EU to jurisdictions outside the U.S. (e.g., data transfers from Europe to Asia, Latin America, and other regions and jurisdictions). Model Contracts also are not subject to enforcement by the U.S. Federal Trade Commission, and rely exclusively on local enforcement by data protection authorities and courts in the European Union. Model Contracts have certain disadvantages relative to Safe Harbor, including that a proper implementation requires the execution and maintenance of a network of intercompany privacy agreements between and among affiliates worldwide. Acquisitions or other corporate changes will trigger requirements to execute new agreements, and changes in business processes or data transfers can also require adjustments to the existing intercompany framework. In addition, the specific terms in the Model Contracts (which sometimes can be difficult to understand and follow) cannot be changed in any way without triggering a data protection consultation or approval requirement and subsequently creating a risk that the agreements will not be recognized by such authority as a valid implementation of the “model” agreement. Finally, among the other terms, the Model Contracts contain express third-party beneficiary rights for the data subjects to sue the EU affiliate (as “data exporter”) and, in certain circumstances, the U.S. parent (as “data importer”) for violations of the terms of the contract. There are no precise numbers of companies that utilize Model Contracts to protect international data transfers, although the “pre-approved” nature of the agreements and their longstanding availability, combined with experience, suggests that they have been used at least as frequently as Safe Harbor to protect data transfers to the U.S.

3. Why would a U.S. company select the Safe Harbor?

U.S. companies may choose to join the Safe Harbor for a variety of reasons. Several of the key driving factors may include:

i) Increased demands for cross-border data transfers. U.S. companies are experiencing increased demands for cross-border data transfers, such as:

(a) greater integration of global business operations,
(b) consolidation of information technology infrastructure and support services,
(c) implementation of company codes of conduct and whistleblower hotlines,
(d) increased requirements to conduct global internal investigations, and to respond to government inquiries and e-discovery and litigation demands on a worldwide basis.

ii) Increased scrutiny of data transfer practices. U.S. companies are also finding that relevant stakeholders are engaging in increased scrutiny of company privacy practices, including works councils and other employee-representative bodies, individual employees, data protection authorities, consumers, competitors, and others. This requires the companies to select and implement reliable solutions for international data transfers.

iii) More flexibility for onward transfers where required by U.S. law, ordered

See, U.S. - EU Safe Harbor, page 6

PRIVACY PREDICTIONS -2010-

Widespread adoption of the icon for online behavioral advertising will occur and be visible across the Internet. Progress on important legal and policy issues will occur if all interests continue to work constructively together. The public will call for more aggressive use of personal information to protect citizens against terrorism. Technology and the Information Age will reach new heights with wireless and television innovation and benefits that rely on consumer information. Public love for the Internet continues to reach new peaks.

—Benita Kahn, CIPP, Partner, Vorys, Sater, Seymour and Pease LLP

—Stu Ingis, Partner, Venable LLP
PRIVACY PREDICTIONS
-2010-

A n arousing turn of the year in the matter of privacy: At the end of 2009 Eric Schmidt, CEO of Google, told CNBC: “If you have something you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.” At the beginning of 2010, Mark Zuckerberg, founder of Facebook, told a live audience that if he were to create Facebook again today, user information would be public by default, not private as it was for years until the end of December.

It seems that privacy has become a disused concept. The new decade is about openness and total disclosure. Individuals and organizations will have to engage even more in protecting privacy as a rare but necessary concept for human life in the digitally networked world. Remember? Privacy has always been interpreted as a precondition for human self-determination and a free and democratic society. I don’t remember any convincing argument that has made this assumption obsolete. So let’s take care.

—Miriam Meckel, Managing Director, MCM-Institute, University of St. Gallen Switzerland, and 2009-2010 Berkman Center for Internet and Society fellow

by a court, or necessary to perform a contract. Safe Harbor has more flexible rules than Model Contracts with respect to onward transfers to third parties. Specifically, Model Contracts prohibit the relevant company from disclosing data to third parties unless it has obtained the agreement of the recipient to abide by the Model Contract terms, or has obtained consent from individuals. Such rules may be difficult for a company to satisfy fully in the context of U.S. government demands for data, court orders in e-discovery or litigation, or data transfers that are necessary to perform a contract with the individual data subject. Similarly, the specific rules on such onward transfers in BCRs need to be negotiated on a case-by-case basis with the European data protection authorities, and may likewise be difficult to satisfy depending on the outcome of such negotiations. In contrast, the Safe Harbor provides important exceptions to onward transfer restrictions, such as for situations where the data sharing is required by a legal requirement in the U.S. (e.g., in the context of government demands for data), a court order in the U.S. (e.g., the context of e-discovery), and data sharing that is necessary to perform a contract with the data subject, or otherwise qualifies for exceptions in the Directive or national data protection laws.

iv) Greater control for the U.S. company. Safe Harbor provides the U.S. company (versus local affiliates) with greater control over the cross-border data transfer solution than Model Contracts and BCRs. The Safe Harbor primarily requires the U.S. company to undertake relevant compliance steps, and does not generally require significant local affiliate involvement. In contrast, Model Contracts require the participation of local affiliates in Europe to execute the intercompany agreements. On an ongoing basis, Model Contracts by their own terms provide local affiliates with audit and other rights over the U.S. companies (a situation that often does not represent the actual hierarchical structure of a U.S.-based company and its local affiliates). BCRs require even more extensive participation of local affiliates to negotiate for substantive approvals from data protection authorities for the terms in the BCRs.

v) Achievable and practical nature of Safe Harbor. Safe Harbor is an achievable and practical solution because, unlike BCRs, self-certification to Safe Harbor does not require any substantive negotiations with the European data protection authorities—the U.S. DOC already completed such negotiations for the Safe Harbor rules several years ago.

vi) Enhanced brand reputation for outsourcing providers and satisfaction of EU customer requirements.

Outsourcing service providers in the U.S. may find Safe Harbor participation advantageous when doing business with corporate customers in the EU (EU Customers). Among other benefits, Safe Harbor participation can help enhance the U.S. provider’s brand reputation, and demonstrate to EU Customers that the provider understands EU data protection concerns. Safe Harbor participation can also help reduce the compliance burden on the EU Customers by helping them avoid the need to maintain a network of Model Contracts conforming to the European Commission “data processor” clauses. In addition, Safe Harbor participation can streamline the steps that the EU Customers need to take to comply with local data protection authority registration requirements in some countries (discussed further below in paragraph vii).

vii) Coverage for Switzerland. The Swiss Federal Data Protection and Information Commission (Swiss DPA) has recently established the U.S.-Swiss Safe Harbor Framework with the U.S. DOC. As a result, U.S. companies can address the cross-border data transfer restriction in the Swiss data protection law by self-certifying compliance to the Safe Harbor rules, in the same way as can be done for transfers from the EU. This development is particularly impor-
tant for Switzerland, as the definition of “personal data” under Swiss law covers identifiable information regarding individuals and legal entities, making personal data protections provided under Swiss law broader than those of many EU member states, which generally only protect identifiable information regarding natural persons.

viii) Better fit for “online” data collections. The Safe Harbor is better suited to protect online transfers of data because the U.S. company would not need to obtain an express consent from Web site visitors for the data transfers, and would not need to enter into contracts with entities in the European Union (both of which may be cumbersome depending on the business model or application). Instead, the Safe Harbor would require the U.S. company to confirm that its privacy policy and privacy practices adhere to the Safe Harbor rules—a step that may be easier for companies to administer in the online context than obtaining Express Consent or executing Model Contracts.

ix) Streamlining of local filing procedures. In a number of EU member states, cross-border transfers of EU Personal Data may trigger registration requirements with the data protection authorities. In some of these countries, the Safe Harbor facilitates the local registration process by avoiding “procedural” approvals that apply to use of Model Contracts and the “substantive” approvals for BCRs. For example, in Spain, the use of Model Contracts attracts certain requirements for special notary and other procedural approvals when the local company registers with the data protection authority. This requirement is not triggered when the data recipient is a U.S. company that self-certifies with the Safe Harbor.

x) Avoiding administrative burdens of maintaining Model Contracts. Model Contracts must be monitored to make sure that they reflect changes in the relevant company’s structure. By contrast, particularly in the context of mergers and acquisitions, as well as other business changes and developments, Safe Harbor avoids the administrative burden of negotiating and executing new Model Contracts to cover new affiliates and data flows.

4. Why would a U.S. company choose a data transfer solution other than the Safe Harbor?

Although there are many good reasons to join Safe Harbor, or use Safe Harbor as a baseline to authorize certain data transfers, there are good reasons why Safe Harbor may not be sufficient for all data transfers, and why a company might choose alternative approaches.

i) FTC enforcement. The promise to comply with Safe Harbor is ultimately subject to the enforcement authority of the FTC. The FTC has recently taken its initial enforcement actions pursuant to the Safe Harbor. In the first case, the FTC obtained a Temporary Restraining Order (TRO) in the United States District Court for the Central District of California enjoining a consumer electronics company (Consumer Electronics Company) from engaging in a broad range of unfair and deceptive practices related to online consumer sales, including misrepresenting that the company participated in Safe Harbor. According to the FTC complaint, the Consumer Electronics Company had, at various times, advertised on its Web sites that it had self-certified to the Safe Harbor, even though it had never done so. The FTC complaint also alleges that the company had engaged in a wide variety of other unfair and deceptive practices relating to commercial practices, such as: (i) failing to notify consumers

See, U.S. - EU Safe Harbor, page 8
I

 Privacy in the healthcare sector, 2010

The concept of de-identified data as a privacy protection will be challenged by multiple stakeholders; the results of this discussion will be critical to healthcare privacy and related federal laws (e.g., HIPAA, HITECH). There will be those who are concerned about the risk of re-identification, there will be those espousing de-identification as being more protective of patients than handling protected health information (PHI) directly and while accomplishing the same goals, and there will be regulators involved in trying to find common ground that satisfies conflicting interests. Ultimately, I suspect that de-identified data will prevail as a better alternative to using PHI in the healthcare sector, albeit with a more regulated security network around it.

—Kim Gray, Chief Privacy Officer, Americas Region, IMS Health

In the field of advertising in 2010, the mobile Internet will finally become the new frontier for user data collection and analysis, and the use of Flash cookies on the Web will likely re-ignite the debate on third-party tracking devices.

—Fernando Bermejo
Associate Professor of Communication at Universidad Rey Juan Carlos in Madrid, Spain and 2009-2010 Berkman Center for Internet and Society fellow

U.S. - EU Safe Harbor

continued from page 7

about applicable customs duties and other taxes; (ii) frequently shipping products that did not comport to customer orders and that had power chargers that were incompatible with local power systems where the consumer was located; (iii) delivering user manuals and electronics controls that were in Spanish or Chinese entirely; (iv) charging consumer credit cards without providing the products ordered; and (v) failing to disclose warranties and other material terms. In addition to the TRO, the FTC seeks further relief in the form of a permanent injunction, restitution, disgorgement of profits, and other equitable relief.

In a second set of enforcement actions, the FTC agreed to settle cases with six U.S. businesses that allegedly falsely claimed that they participated in Safe Harbor. The FTC complaints charged World Innovators, Inc.; ExpatEdge Partners LLC; Onyx Graphics, Inc.; Directors Desk LLC; Collectify LLC; and Progressive Gaitways LLC (the “Safe Harbor Six”) with representing that they held current certifications to the Safe Harbor program, even though the companies had allowed their certifications to lapse. Under the proposed settlement agreements, the Safe Harbor Six are prohibited from misrepresenting the extent to which they participate in any privacy, security, or other compliance program sponsored by a government or any third party. The FTC did not assess any fines in connection with these settlements.

These cases are important because they represent the first enforcement actions the FTC has taken under Safe Harbor since the inception of the program in November 2000. It may signal that the FTC will be more active in pursuing Safe Harbor cases in the coming months, and that companies should be even more diligent in confirming that they comply with the Safe Harbor rules before completing a self-certification.

ii) Data transfers not eligible for coverage by Safe Harbor. U.S. companies are only eligible to join the Safe Harbor to protect certain transfers of EU Personal Data to the United States. Other transfers within a global enterprise, such as transfers from the EU to Asia or Latin America, are not covered by Safe Harbor. Likewise, financial institutions and other organizations that fall outside the scope of FTC and DOT authority are not eligible to join Safe Harbor, even if the organizations are located in the United States. This “coverage” issue is perhaps one of the most significant reasons why companies may utilize other approaches.

iii) Development of tailored privacy compliance programs. U.S. companies that already have well-established global data protection programs may wish to consider developing more tailored company-wide data protection compliance programs through BCRs. Such companies can build on the controls that they have already established under Safe Harbor and/or Model Contracts, and develop rules and procedures that address the guidance issued by the data protection authorities on BCRs, while tailoring such terms to the group’s actual data flows and handling practices. In the interim period while the group of companies seeks approval for BCRs, they can continue to rely on their existing data protection framework.

5. What are the current trends in international data transfers?

Although there are still a wide variety of practices, certain trends are emerging with respect to international data transfers. First, common industry practice has moved away from reliance on a broad “waiver” of privacy rights through Express Consents, particularly in the employment context. Second, although BCRs are up and coming, the burdens of negotiating for substantive approval from data protection authorities and other factors may place this solution out of reach for many U.S. organizations, except for companies that already have well-developed global privacy programs based on Safe Harbor or Model Contracts.

Third, the “work horses” for compliant international data transfers in the cur-
rent environment appear to be Safe Harbor and Model Contracts. Companies entering the “global privacy compliance” market for the first time at the enterprise level often select between these two solutions. Key considerations in favor of Safe Harbor include more flexibility with respect to onward transfers (e.g., to government authorities in SEC or other government investigations, as well as to other parties in e-discovery and litigation), greater control for the U.S. parent company, the avoidance of the maintenance of a network of intercompany privacy agreements, and the avoidance of express third-party beneficiary rights for data subjects. Key considerations in favor of Model Contracts are the avoidance of FTC enforcement authority, and the ability to cover data transfers from the EU to non-U.S. jurisdictions (e.g., Asia or Latin America).

Ultimately, there is no one-size-fits-all solution. Companies make strategic decisions on cross-border privacy solutions based on their own particular situation, including worldwide data flows, compliance issues, business operations, litigation experience, and other factors. One trend that is unmistakable, however, is that companies today operate in an increasingly interconnected world and, for enterprise risk management purposes, are finding that, at a minimum, they benefit from a periodic review to confirm that the global “privacy house” is in order and responsive to the latest risks and privacy regulatory developments.

Brian Hengesbaugh, CIPP, is a partner in the Chicago office of Baker & McKenzie. He concentrates on domestic and global data protection, privacy, and information security, and is a member of the firm’s Global Privacy Steering Committee. Mr. Hengesbaugh is a past member of the IAPP Publications Advisory Board. Prior to joining Baker & McKenzie, Mr. Hengesbaugh served as the lead attorney for the U.S. Department of Commerce General Counsel’s Office in the negotiation of the U.S. - EU Safe Harbor Privacy Framework.

Michael Mensik is a partner in the Chicago office of Baker & McKenzie, concentrating on information technology, sourcing, and privacy. He was recently elected to the Outsourcing Hall of Fame by the International Association of Outsourcing Professionals.

Amy de La Lama is a senior associate in the Chicago office of Baker & McKenzie, concentrating on domestic and global data protection, privacy, and information security.