EU-U.S. Data Flow: An Unstable Connection

Axel Spies and Thomas Bookwalter

Dealing with conflicting privacy rules is like fitting a U.S. plug into European wall sockets.

Americans cite privacy as a top concern in the 21st century—ahead of overpopulation and racial tension. That may be because they're growing aware of the increasing use of ecommerce and massive computer storage capabilities in ways that raise privacy concerns. Common, even accepted U.S. practices include:

- "Check the box" agreements to sales of personal data to third parties.
- Installation of "cookies" on customer's computer hard drives.
- Bombarding customers with carefully targeted but unwanted ads.

Until very recently, U.S. government regulation of such activities was very limited, and even what we have now targets very specific situations. The result has been a hodgepodge of *ad hoc* company policies and small print on websites.

While often sufficient for U.S. regulatory purposes, such practices generally are not satisfactory to European Union (EU) regulators. The fundamental differences between U.S. and European privacy policy can no longer be ignored.

The EU takes its "mission" literally. The Union's 1995 Data Protection Directive prohibits the transfer of personal data to non-EU nations that do not meet the European "adequacy" standard for privacy protection. This Directive defines "personal data" broadly as any information "relating to an identified or identifiable person" (not only covering addresses, but also, for instance, fingerprints, x-rays, photos, license tags).

The EU has identified the U.S. as a country that fails to offer "adequate" privacy protection, and has threatened to halt personal data flows from the EU to the U.S. This article attempts to help U.S. technology managers understand the implications of the rift between the U.S. and EU over privacy standards and provide some guidance about what to do.

Directive On Data Protection

The European Commission's Directive on Data Protection is the key document in EU privacy protections and regulations. The terms "data protection" and "data subject" in this document reveal the EU's philosophy: It's the responsibility of government to protect the personal data that companies are using.

Each EU member state has one or several "Data Protection Agencies" (DPAs) to ensure this is done. The DPAs have their own investigative tools and sanctions. They may even shut down servers or impose hefty fines. Moreover, in-house data protection officers in all larger European companies support the data protection agencies in their activities.

The DPAs in each country monitor, investigate and enforce privacy laws at their own discretion. In addition, privacy watchdog groups and other organizations may file complaints to trigger investigations. The German DPA in Hamburg recently announced, for instance, that it has developed software that will automatically search and identify websites that do not comply with data protection law. The French DPA ("CNIL") requires each ISP collecting personal data to file a questionnaire with CNIL. The ISP must also make detailed statements to CNIL about its privacy policy and inform the user as well.

Since uninterrupted flow of personal data between the EU and the U.S. is critical, U.S. companies must address the EU requirements if they wish to continue to do business in Europe. The question is how.

Dr. Axel Spies is foreign legal consultant at Swidler Berlin Shereff Friedman, LLP, a law firm which handles U.S. and international telecommunications law. Thomas Bookwalter is president of LYNX Technologies, Inc. which advises carriers and enterprises regarding telecom services. LYNX publishes the Global Telecommunications Database and PriceConnect for foreign private line pricing over the Internet.

TABLE 1 The Seven Safe Harbor Principles

(1) NOTICE: Let the public know what you are collecting and what you are doing with it.

(2) CHOICE: Let the individual choose whether his or her personal information is disclosed to third parties.

(3) ONWARD TRANSFER: Only pass on collected personal data to third parties protecting privacy adequately.

(4) SECURITY: Keep personal data safe all the time.

(5) DATA INTEGRITY: Keep personal data accurate, complete and current.

(6) ACCESS: Enable individuals to check, correct, amend or delete their personal data.

(7) ENFORCEMENT: Set up an efficient internal or external mechanism to assure compliance with the Safe Harbor Principles; provide for dispute resolution, remedies and sanctions.

No Safe Harbor From The Storm?

The EU and U.S. want to bridge the policy gap on privacy protection. They're trying to find a middle ground between the U.S.'s "bottom-up" approach of reliance on industry self-regulation and the European "top-down" approach of government-enforced policy. Toward this end, the U.S. Department of Commerce and European Commission developed a "Safe Harbor" concept last year.

This concept consists of a set of rules (the "Principles" and the answers to Frequently Asked Questions or "FAQs;" see Table 1). U.S. companies may voluntarily agree to implement these principles in order to be deemed in compliance with EU privacy protection regulations for transborder personal data flow to the U.S.

The Safe Harbor concept was trumpeted as a landmark accord for ecommerce. In practice, few U.S. companies have formally adopted the rules, among them only a handful of large corporations, such as Level 3, Hewlett-Packard, Intel and Dunn & Bradstreet.

One reason companies do not sign on to the Safe Harbor Principles is fear of exposure to legal risks in the U.S. and abroad. The EU agreed to accept the Safe Harbor Principles only because enforcement provisions were included: The Federal Trade Commission, and for a smaller number of companies the Department of Transportation, can sue companies that violate their commitments to live up to the Safe Harbor Principles.

However, some companies fear that an EU member state or national DPA may refuse to recognize a listed company as a "Safe Harbor company." In fact, a recent study of 75 websites of U.S. multinational companies found that none of the websites reviewed met all the standards required by the Safe Harbor Principles. For instance, only 5 percent had set up enforcement provisions for consumers. Finally, some business sectors, such as the financial sector, are not covered at all by the Safe Harbor Principles. This means that financial institutions do not have the option to use Safe Harbor Principles as a way to bypass compliance with the more rigorous standards of the EU and DPAs.

Finding The Right Data-Flow Plug

What are the alternatives to adhering to the Safe Harbor principles?

A company could simply ignore the problem. In fact, this is what many U.S. companies are doing. However, in view of the possible sanctions that European data protection agencies (and/or individuals) may impose, this is a potentially dangerous approach that puts a company's ability to continue to operate effectively in Europe at risk.

Claiming "not to know" may not prevent the EU or a DPA from requiring a U.S. company to stop its flow of "personal" data from Europe to the U.S. while it implements its solution. The extent to which a company would be sanctioned depends on national law, but it would at least extend to closing down its Web-based customer services, imposing penalties and even launching a criminal investigation. The business losses could be significant, not to mention the penalties.

The other extreme is seeking the explicit consent of each individual from whom personal data is collected. However, this approach may pose insurmountable practical and logistical obstacles. For example, while the "I Agree" button is accepted in the U.S. as sufficient, under EU standards it is not. This is partly because it is difficult to provide sufficient evidence that it was actually the individual, the "data subject," who has clicked on a button on a website.

If a U.S. company doesn't find either of the two extremes appealing, it may submit its privacy policy to each DPA for prior approval. The approach looks simple in theory: A company representative contacts the offices of the national DPA in charge of the region where data are collected, presents the company's approach to data security to the staff and obtains the blessing of the data czars.

While this approach might have worked in some individual cases, it is simply not feasible for an international corporation. The approach of a data czar in Athens may differ from that of a data czar in Helsinki. Official policy approval may be necessary and may take months if not years. In the meantime, the company might find itself in a legal quagmire of conflicting national regimes and endless discussions with multiple officials, and potentially the inability to move personal data anywhere.

There is a "safe harbor" but it's rarely used

The Universal Adapter?

The European Commission recently suggested another compliance method. Last June, the Commission released a document commonly referred to as the "EU Standard Clauses." It is actually a detailed contract that the European Commission praises as a "useful tool."

Unfortunately, the EU Standard Clauses do not look good even on paper, much less in practice. They are full of unclear, sometime dangerous terms that may carry substantial risks: For example, U.S. companies receiving personal data could be sued in Europe by individuals for breach of the EU Standard Clauses if the transferring entity allegedly mishandles the data.

TABLE 2 Powers Granted European DPAs

- Ask for detailed information.
- Publish unfavorable reports.
- Demand copies of electronic information.
- Search on the premises and seize printed and electronic information and hardware.
- Disrupt or suspend personal data flows of a company.
- Impose hefty administrative fines and ask courts for criminal penalties (fines and/or imprisonment).

A company can create its own privacy policy, but this risks alienating the authorities

European business partners and/or European DPAs will probably urge at least those U.S. companies that have not agreed to the Safe Harbor Principles to implement the EU Standard Clauses. The U.S. government, however, has already expressed strong reservations about the Standard Clauses and is reviewing its options. Interestingly, the U.S. is backed in its position by some national DPAs, who fear that the European Commission is encroaching on their turf.

Recently, a group of international trade associations released its own proposed Standard Contractual Clauses for the transfer of personal data from the EU to "Third Countries." These are somewhat less bureaucratic than the EU Standard Clauses, but they also contain burdensome provisions. For instance, the entity importing the personal data outside the EU can be requested to provide evidence that its financial resources are "sufficient for purposes of processing data" under these Standard Contractual Clauses.

In order to avoid the Standard Clauses, some international players, in particular large corporate groups, prefer to define a detailed group-wide Global Privacy Policy. They create their own set of privacy rules defining a system that suits their own needs by embodying flexible provisions to deal with transnational data flow.

For instance, companies provide for a complaint mechanism, an internal dispute resolution mechanism and describe in reasonable terms what they do and what they will not do with the personal data. They lobby for their "sector-specific" policy through their industry representatives in Europe. If a national DPA is unhappy with a certain provision, the company addresses the problem without undue delay by amending its policy or modifying the relevant provision.

This "common sense" approach is not without risks. Showing good intentions is not identical with actual compliance with the law. A DPA may get upset that "its" national policy on data protection is not exactly mirrored by the company policy, and may initiate a proceeding. In addition, developing a Global Privacy Policy requires a significant amount of work and expense. Many companies shy away from this.

How The Plug Is Attached

The Safe Harbor Principles, the EU Standard Clauses and the recently proposed industry Standard Contractual Clauses all provide for verification mechanisms to ensure that the company actually implements the privacy policy it has committed to. For example, the rules on an annual compliance review under the Safe Harbor Principles include the following steps:

- Determine which means of certification you will use. Annual certification is required under the Safe Harbor Principles, and the authorities permit either external or self-certification.

External certification uses an authorized third-party certifier to review your current compliance with the Safe Harbor Principles and to certify your company when you have met the standards of the Safe Harbor Agreement.

In self-certification, a company establishes an internal certification capability that performs the review and certification. While this might sound preferable to submitting to an outside certifier, bear in mind that an officer of the company seeking certification must sign a statement verifying compliance, thus assuming legal responsibility for the veracity of the certification. Therefore, a good approach to Safe Harbor Compliance is to complete the initial certification with an independent external third-party company and then conduct annual reviews internally.

- Examine the existing organizational environment. Compliance with the Safe Harbor Principles is achieved through a combination of systems features, company policies, information management practices, training of staff about the Safe Harbor Principles and the creation of a system for handling complaints and inquiries. The company is evaluated in all areas, and a baseline level of current compliance is defined.
- Perform a gap analysis. Once the existing environment is defined, a gap analysis is performed to identify discrepancies between the existing policies and the requirements of the EU and DPAs.

Using the variance as a guideline, specific steps are defined to bring your company into compliance with the Safe Harbor Principles, and to demonstrate that compliance to the authorities. The analysis will also reveal those regulations that will be too difficult or costly to resolve; these problem areas will need to be discussed with the various regulators.

- The last step in the process is to develop and implement a plan to meet the requirements and complete certification.

Conclusion

There is no clear-cut solution for every company. The environment is still only roughly defined, but the EU countries continue to move forward on rules. Given the time required to implement solutions, waiting may have substantial downside risk for companies operating in Europe.

As a first step, a privacy team of in-house and external experts should review the current situation and make suggestions on how to enhance data protection. In particular, the company should be leery of personal data not obtained directly from an individual.

This process has several benefits: It goes a long way toward satisfying the European DPAs, which have extensive powers to impose sanctions on the company. Secondly, it enhances customer confidence by ensuring privacy rights in a global commerce environment. There are, for instance, privacy seal programs available for this purpose, the best-known of which is TRUSTe, http://www.truste.org/. The investment into privacy protection, a prime concern of consumers, will pay off□