

**WR&F's**  
***Privacy In Focus***  
**MARCH 2001 ISSUE**

### **EC Produces Disappointing Draft Model Contract Privacy Clauses**

The European Commission ("EC") recently released draft model contractual clauses that lay out certain privacy obligations. EU firms and their trading partners may secure certain protections if they incorporate this set of clauses into contracts involving personal data transfers from the European Union. The EC's draft language is currently before the European Parliament as well as an EC committee composed of representatives of the 15 EU member states. A decision on whether to accept the draft is expected as soon as the end of March.

### **Objectives of the Model**

Conceptually, the model contract language could benefit U.S. firms importing EU personal data by providing a ready and predictable basis for personal data exports, but, unfortunately, the current draft imposes significant burdens and risks. If adopted without modifications, it may fail to provide a viable option. The Safe Harbor agreement administered by the U.S. Department of Commerce will likely provide a more congenial alternative for most U.S. businesses. On a broader level, the model clauses demonstrate the continuing tension between the U.S. and EU approaches to privacy protection. With some exceptions, the EU Directive on Data Protection ("Directive") prohibits the transfer of personal data to nations, like the United States, where privacy protection is not deemed "adequate." Currently, U.S. firms have only three options for establishing "adequacy": (1) join the Safe Harbor program; (2) tailor operations to fall into an exception to the Directive; or (3) obtain approval from EU member state data protection authorities ("DPAs") for specific personal data transfers. The Directive envisions model privacy contracts as an additional option and delegates responsibility for drafting standard language to the EC.

Ideally, an EU-wide model contract would provide a single standard of "adequate" privacy protection, as opposed to the varied laws of the 15 EU member states. The EC draft decision, however, leaves with member states the discretion to impose requirements beyond those in the model clauses. For example, a member state may increase the extent of disclosure and the degree of specificity required within a model contract, and it may restrict the cases in which an EU-based data exporter may transfer data under a model contract. Consequently, companies could face fifteen separate sets of transfer requirements despite their use of the model contract language. In contrast,

## *Wiley, Rein & Fielding*

under the Safe Harbor agreement, firms generally must comply with only the single standard defined by the Safe Harbor Principles, which is binding on the member states.

### **Liability and Enforcement**

The liability provisions of the draft contract raise the greatest concern. The clauses provide that the EU-based data exporter and the U.S.-based data importer are jointly and severally liable for breach of the contractual provisions. EU data subjects, the individuals identified by the data transferred under a model contract, are named as third party beneficiaries of most privacy provisions and may bring a civil action against either party for damages. Moreover, an “association” of plaintiffs may bring third party beneficiary suits. Neither the Directive nor the Safe Harbor agreement includes these liability provisions.

The model contracts exceed the requirements of the Directive in other significant ways. The Directive requires that data be kept for no longer than necessary, but the model contract requires firms to commit to a date by which the data will be destroyed. The draft clauses require notice to individuals when their “sensitive data,” such as health or ethnicity information, will be transferred under a contract; the Directive requires no additional notice once individuals give their consent to the data’s collection, use and transfer. These privacy protections will survive the termination of the contract.

The model clauses significantly erode the ability of businesses to bargain for key contract terms, with the consequence that U.S. parties to a model contract must submit to EU member state law, EU forums and EU regulatory authority. Parties to a contract may not elect to resolve disputes under U.S. law; a member state’s legislation must serve as the governing law of the contract. U.S. data importers must agree to cooperate with DPA inquiries (which may include privacy audits), to file their contracts with DPAs, and to follow DPA “advice” regarding data processing. Member state DPAs may prohibit or suspend data transfers based on their interpretation of standard contractual clauses. EU data subjects have the right to bring actions under the laws of their home state for compensation for damages suffered. If a non-judicial dispute resolution procedure fails to satisfy the data subject, he or she would retain the right to bring a court action in the EU. Again, the Safe Harbor is significantly different—EU individuals seeking redress from U.S. companies must bring most privacy disputes before a U.S. self-regulatory dispute resolution body chosen by the U.S. data importer.

Additional risk arises under the model contract scheme, because constraints on DPA action are weak, even if a firm adheres to the contractual provisions. Model clauses may be amended at any time, and the draft EC decision does not specify whether such amendments might have retroactive effect. DPAs may order suspension of personal data flows to a U.S. party in a variety of circumstances, including a DPA’s belief that a substantial likelihood exists that a model contract will not be complied with and a breach would cause an

***Wiley, Rein & Fielding***

imminent risk of grave harm. DPAs also have the power to judge that the tenets of U.S. law conflicting with contractual privacy protections are not “necessary in a democratic society” and will not excuse a breach.

### **Broader Concerns**

The model language clearly represents a retreat from the flexible approach to defining “adequate” privacy protection underlying the Safe Harbor agreement. The stringency and extra-territorial reach of the draft model contract language may be an attempt to stiffen the definition of “adequacy” and increase the EU’s leverage vis-a-vis other third-country data recipients, as the DPAs who drafted the model clauses intend them to establish a “reference document for future developments on data protection in the international field.” The draft model contract may thus suggest challenges ahead for businesses located in the U.S. or elsewhere that are dependent on personal data flows from the EU.

For additional information on the Draft Model Contract Privacy Clauses or the U.S.-EU Safe Harbor program, please contact John Reynolds (202.719.7342 or jreynold@wrf.com) or Amy Worlton (202.719.7458 or aworlton@wrf.com). n

### **HIPAA Privacy Rules Up in the Air**

As covered health care entities begin to struggle with the complexities of the HIPAA privacy rules that were finalized in December 2000, recent actions by the Department of Health and Human Services (“HHS”) have thrown the future of these rules into question.

First, HHS announced that the effective date of the rules would be postponed until April 14, 2001, due to a failure by the Clinton administration to communicate the substance of the regulations to Congress. This requirement, stemming from the Congressional Review Act, mandates that Congress have notice of “major” rules and a period of time to review such rules. In another instance, this “speedy review” process recently resulted in overturning an agency rule issued by the “lame duck” Clinton administration, the controversial Occupational Safety and Health Administration “ergonomics” rule.

### **Comment Period Reopened**

With that modest extension of the HIPAA rules’ effective date (from the original February 26, 2001 date), HHS also has reopened comments on the substance of the final rules, with comments due by March 30, 2001. In announcing this new comment period, HHS Secretary Tommy Thompson said that the delay in the effective date “creates an opportunity to ensure that the provisions of this final rule will indeed work as intended throughout the complex field of health care, without creating unanticipated consequences that might harm patients’ access to care or quality of care.”

There is a widespread debate as to whether this new comment period will result in significant changes to the rules. Secretary Thompson has indicated that HHS’ goal “is to achieve privacy protection that works.” He has stated that HHS “should be open to the concerns of all those who care strongly about health care and privacy.” With the new effective date only 14 days after the expiration of the comment period, the health care community may learn in early April the preliminary fate of these rules. Thompson has stated that HHS’

commitment “must be to put strong and effective patient privacy protections into effect as quickly as possible.”

### **Arney Questions Rules**

House Majority Leader Dick Arney has thrown his voice into this debate, expressing concern because the rules allow the U.S. Government too much access to health care information (primarily through the provisions that allow HHS access to patient information in monitoring compliance with the rules). His position may add to the pressure on HHS to revise substantively the content of the privacy rules.

*Privacy in Focus* will report next month on any changes resulting from this comment period. In the meantime, for any questions on these issues, please contact Kirk Nahra (202.719.7335 or [knahra@wrf.com](mailto:knahra@wrf.com)). n

### **Second in a Series**

### **Organizational Models for Integrating the Privacy Officer Function Throughout a Diversified Company**

In the February 2001 issue of *Privacy In Focus*, we identified considerations that are central to the implementation of a business entity privacy program. In particular, as to the appointment of a Chief Privacy Officer (“CPO”), we analyzed such key questions as: should you designate a CPO at all; *when* should you designate a CPO; and *where* in the corporate structure should you place the CPO function?

In examining this last question—where in the corporate structure should the CPO fit—we focused on the CPO’s upward reporting relationship, not on how a company can ensure that the Privacy Officer successfully influences operations throughout the company. This latter challenge—weaving the Privacy Officer into the fabric of a company—is particularly significant and is complex, especially for the highly diversified company.

### **Highly Diversified Company**

Many large companies have multiple business (or product) lines, with each business/product line established as a separate division or subsidiary, or where the different business/product lines are dispersed among various subsidiaries. An example of such a highly diversified company would be an insurance holding company that has established separate subsidiaries to independently provide: health insurance products for fully-insured health plans (or administrative services for self-insured health plans); life insurance

## *Wiley, Rein & Fielding*

products; coverage for workers' compensation claims; and property and casualty insurance coverage. Although each of these product lines is separate and distinct, personal information may flow among the various subsidiaries.

Consequently, the parent company of such an organization understandably will have a strong interest in ensuring that its privacy obligations and related policies are understood and appropriately implemented by *all* employees within *all* operating units and subsidiaries. What organizational tools can best help the CPO to establish and maintain top-to-bottom compliance with the company's privacy obligations and policies? We describe below two basic organizational models that companies may wish to consider to facilitate the integration of the CPO function throughout a diverse corporate structure.

### **The Privacy Committee**

One model revolves around a "Privacy Committee." Although a Privacy Committee can assume different functional roles, it is usually a committee comprised of representatives from key (or all) divisions or subsidiaries and/or from key (or all) business/product lines within the subsidiaries. This model is designed to foster a cooperative, integrated effort among the operational stakeholders at various levels who will implement a company's privacy policies.

The Committee could operate as a single, democratic collective voice (*i.e.*, embracing the concept of the majority rules), with the Chief Privacy Officer acting as a member of the Committee (albeit the organizer and facilitator). Alternatively, the Committee could serve in an advisory capacity to the Privacy Officer.

The scope of the Committee's charge will depend on the character of the privacy initiative within the company, and on the staffing, financial resources and administrative support provided to the Privacy Officer. Depending on these considerations, the Privacy Committee could serve as a reviewer of the company's substantive privacy program, as well as procedural and administrative matters arising in its implementation. The Committee also could author or review policies and procedures, training publications and other written materials. Additionally, the Committee could be charged with providing hands-on assistance in the actual implementation of these measures.

A significant advantage of the Committee model (even if purely advisory) is that individuals within different areas of a company (*i.e.*, including multiple subsidiaries), with diverse responsibilities and perhaps with divergent views

## *Wiley, Rein & Fielding*

on the appropriate nature or scope of the privacy effort, can develop an understanding of the company's overall privacy strategy, as well as an appreciation of the application of the privacy program to their particular area. In addition, such an approach allows the Committee members to serve as the first line of defense in identifying implementation or operational issues for the Privacy Officer, and in spotting potential areas of non-compliance. Many highly diversified companies are embracing the Privacy Committee model.

The Committee approach also can be used to facilitate creating (rather than simply implementing) a company's privacy program. At the formative stages of developing the privacy program, the Committee approach is reflected in the establishment of a Privacy Management Office ("PMO"). Included among the matters PMOs typically address are answering many of the questions explored in the February 2001 *Privacy In Focus* discussion, such as the optimum skills for the CPO, where in the corporate structure the CPO function should be placed and whether the company's privacy program should be established as a part of its existing compliance effort. In addition, PMOs can provide the initial inventory and assessment of a company's personal information uses and risks, including particular subsidiary or business/product line issues or concerns that should be considered in developing the privacy program.

Thus, whether at the developmental or operational stages, the Committee model can be an effective organizational tool for implementing privacy policies within a diversified company.

### **CPO and Deputy Privacy Officers**

Another approach highly diversified companies are embracing for effective privacy program implementation is the CPO and Deputy Privacy Officer ("DPO") model. Although, at first blush, this model may seem functionally indistinguishable from the Privacy Committee model, there are differences.

Under the CPO/DPO model, the DPOs are indeed privacy officers, but are located in operating units. As privacy officers, DPOs would be required to have the same kinds of skills as the CPO and would have the same basic duties as the CPO, but for a more narrow sphere. DPOs are placed in key (or all) subsidiaries (or within each operational division housing a distinct business/product line). For each designated oversight area, the responsible DPO serves as the principal privacy officer.

Under the CPO/DPO model, the DPOs report to the CPO, who is principally responsible for ensuring uniformity in the application of the company's privacy

## *Wiley, Rein & Fielding*

policies and uniformity in the general implementation of the company's privacy program. Thus, this arrangement is more hierarchical and less democratic than the Privacy Committee model.

The CPO/DPO and Privacy Committee models are not mutually exclusive. Thus, for example, a company may establish a Privacy Management Office to coordinate the creation of the privacy program (or until a CPO is selected). Thereafter, the company could implement the CPO/DPO model. Alternatively, a company could have a CPO/DPO model as its principal privacy program implementation vehicle, and also have a Privacy Committee comprised of operational stakeholders to serve in an advisory capacity to the CPO/DPOs. What may prove to be the most appropriate model for any given company will depend on such factors as the diversity (substantively and organizationally) of its operations, the resources available and the scope of its privacy program obligations and goals.

For more information on the role of privacy officers, please contact Dorthula H. Powell-Woodson (202.719.7150 or [dpowell-woodson@wrf.com](mailto:dpowell-woodson@wrf.com)) or Kathryn Bucher (202.719.7530 or [kbucher@wrf.com](mailto:kbucher@wrf.com)). n

### **WRF Speakers to Appear at Privacy Officers Association National Meeting**

The Privacy Officers Association will host its first annual Privacy and Data Protection Summit on May 2-4, 2001, in Arlington, VA. The program will bring together privacy officers and a wide variety of others from the health care, financial services, e-commerce, government contracting, Internet industries and academia to assess emerging privacy and data protection issues confronting corporate America today.

Wiley, Rein & Fielding attorneys John Kamp and Kirk Nahra will participate in the program. John will moderate the Privacy Officer Roundtable, featuring presenters from Citigroup, FleetBoston, IBM, Doubleclick, Express Scripts and HCA-The Healthcare Company. He also will participate in a session called "A Socratic Dialogue on Privacy Security," moderated by Harvard Law Professor Arthur Miller.

Kirk Nahra will address "Privacy Issues for Insurance Companies," following up on WRF's own January 30-31 conference on Privacy Issues for the Insurance Industry. This presentation will address the primary privacy challenges confronting insurers—the Gramm-Leach-Bliley Act regulations for the entire industry and the HIPAA regulations for health insurers—as well as a strategy for developing a privacy policy that accommodates these separate (and sometimes conflicting) rules.

For more information on the Privacy Officers Association or the Summit, please

## *Wiley, Rein & Fielding*

contact Melissa Horowitz (800.266.6501 or [melissa.horowitz@rmpinc.com](mailto:melissa.horowitz@rmpinc.com)). For information on WRF's participation, please contact Kirk Nahra (202.719.7335 or [knahra@wrf.com](mailto:knahra@wrf.com)) or John Kamp at (202.719.7216 or [jkamp@wrf.com](mailto:jkamp@wrf.com)). [n](#)

### **Industry Engages Privacy Issues at FTC Profiling Workshop**

On March 13, the Federal Trade Commission ("FTC") hosted scholars, privacy advocates, marketing industry representatives and the general public for an in-depth look at consumer profiling, the process of merging data about individuals and their buying habits from multiple sources. FTC Commissioner Orson Swindle kicked off the workshop saying that a "great trust deficit" makes consumers wary about how businesses use their personal data, but at the same time, the free flow of information has great economic value.

Industry representatives provided an unprecedented look into the collection and merging of consumer data in the United States. Public records, market surveys and businesses' customer lists can be merged to create powerful predictors of what goods and services will appeal to individual consumers. Privacy advocates called for notice to consumers that their data could be merged from various sources and for consumer access to records stored by data compilers. Others argued that public records such as land title transfers and voter registration should not be available for marketing purposes without the individual's consent.

### **Profiling Benefits Noted**

Academics and business representatives provided evidence that the free flow of personal information confers significant benefits on the U.S. economy. Readily available data help reduce fraud, lower the cost of credit and encourage competitive entry by helping new businesses find prospective customers. Studies show that information sharing saves the financial sector and apparel retailers billions of dollars a year, resulting in lower prices. More study is needed, they argue, before policymakers will understand the trade-offs between privacy protection and data compiling. It is also unclear whether privacy legislation will actually increase consumer confidence.

Moderate voices on the workshop's panels called for more transparency of profiling activities. "We need much better notice [of data practices]," said Mary Culnan, a professor at Bentley College. "The industry can do a lot to educate people [about] the benefits of profiling and that these benefits outweigh the risks."

For additional information, please contact John Kamp (202.719.7216 or [jkamp@wrf.com](mailto:jkamp@wrf.com)) or Amy Worlton (202.719.7458 or [aworlton@wrf.com](mailto:aworlton@wrf.com)). [n](#)

## **Bankruptcy Legislation Addresses *Toysmart* Issue**

The recent Toysmart.com bankruptcy highlighted a tension between consumers' interests in their privacy and the value of a business' customer list in bankruptcy law. The *Toysmart* case itself was resolved in favor of consumer protection. As we go to press, however, the Senate has inserted into comprehensive bankruptcy reform legislation a specific provision that directly addresses this tension. If the provision becomes law, a new regime would apply to both offline and online businesses.

### ***Toysmart* Outcome**

As discussed in our August 2000 issue, the controversy involving privacy as to individual data contained in a business' customer list and bankruptcy erupted when Toysmart.com—the former “smart toys” web site—attempted to sell, as an asset in bankruptcy, its customer list data. The controversy arose because Toysmart had collected this customer information while it posted a privacy statement declaring that it would “never” share this data with other parties. Toysmart's attempt to sell the customer list as an asset of the bankrupt business was challenged by the FTC, more than 40 state attorneys general and TRUSTe on various grounds ranging from breach of contract to violation of consumer protection and fair trade laws.

In January, Toysmart ultimately concluded that the delay and cost of litigating the matter outweighed any commercial value that the list might have. Therefore, with the consent of the bankruptcy court, it accepted an offer by the Walt Disney Company—one of Toysmart's investors—of a relatively modest \$50,000, in return for which Toysmart agreed to destroy the list without disclosure.

Despite wide publicity, the Toysmart bankruptcy case, strictly speaking, made no law. As the ultimate destruction of the customer list required no transfer to Disney, the bankruptcy court never needed to rule on claims that a sale of the customer list would violate federal or state fraud law, or Toysmart's contract with TRUSTe.

### **Senate Bankruptcy Bill**

Congress, however, is now addressing the tension revealed in this case. The Senate version of the comprehensive bankruptcy reform legislation (S.420) includes a provision addressing the disposition of customer lists in business bankruptcy proceedings. In particular, the Senate version creates an exception to the usual power of a bankruptcy trustee to dispose of a debtor's assets. Under the exception, a debtor could not “sell or lease” personally identifiable information about an individual customer if the debtor had published a privacy statement prohibiting the transfer to unaffiliated third persons.

By “personally identifiable information,” the Senate bill means a person's name, physical and e-mail addresses, home telephone number, Social

## *Wiley, Rein & Fielding*

Security number and credit card number. In addition, other information, including birth date, birthplace, or other information that, if disclosed, will result in physical or electronic contacting of the person also comes under the scope of the Senate bill's protection.

Several important conditions limit the scope of this new exception. First, the privacy statement must remain "in effect at the time of the bankruptcy filing." This implies that a debtor could change its statement on the eve of bankruptcy to evade this limitation. Nor does the Senate bill address whether, in such circumstances, a debtor could sell personal information collected under a previous privacy statement which had promised no sale to third parties.

Second, the bill also would authorize a bankruptcy judge to allow such a sale, despite a past promise not to sell, if circumstances warrant. The bankruptcy court is to weigh the particular representations in the privacy statement, the potential privacy gains and losses to consumers if the sale was allowed, the potential costs and benefits if the sale was approved, and possible mitigating alternatives. At first blush, this provision appears to invite litigation in nearly every dot.com bankruptcy case until a body of precedent is established that gives meaning to the exception.

### **Not Limited to Dot.Coms**

Although the Senate drafters apparently targeted the new provision at failing dot.coms, the bill's scope is actually far broader. The provision appears to apply to any debtor that has "disclosed" a privacy statement "to an individual" where the statement prohibits the sale or lease of the personal information to unaffiliated parties. The Senate bill does not require that the disclosure be via a web site; apparently, a disclosure in a mailing or even face-to-face would suffice. Nor is there any requirement that the individual be aware of the policy, or even that the individual provide the data online.

Thus, this provision potentially could apply broadly to personal information collected offline by a company that had included a privacy statement in a mailing to the consumer. For example, so long as a privacy statement has been disclosed to a consumer, the Senate bill's provision would apply to personal information from consumers collected by a merchant by telephone, by mail, or even face-to-face.

Whether the Senate bill would have much practical effect is unclear. By specifically bestowing additional protection to certain limited categories of personal information, the bill arguably modifies current law by constraining a business debtor's ability to sell its customer lists. However, as the *Toysmart* case shows, the law is unsettled as to whether an online business actually has the right to sell its customer list where it has stated that it would not do so. Nonetheless, by allowing a bankruptcy court to permit such a sale after "due consideration of the facts," the Senate bill may actually produce an outcome no different than the situation today, in which a debtor's ability to dispose of a customer list is, as in *Toysmart*, a matter of litigation.

For additional information, please contact Bill Baker (202.719.7255 or

*Wiley, Rein & Fielding*

wbaker@wrf.com). n

## *Wiley, Rein & Fielding*

### **Upcoming WRF Speaking Engagements**

<b><u>Date</u></b>	<b><u>Speaker, Topic and Event</u></b>
April 26	Meredith Fuchs will present “Privacy Issues for Business” at the Alabama Bar Institute’s 38 <sup>th</sup> Annual Corporate Law Institute, in Point Clear, AL.
April 30	Tom Brunner will present “In the Age of Commerce, Insuring Electronic Risk” at the Alliance of American Insurers’ 79 <sup>th</sup> Annual Meeting: Risky Business Insurance in the 21 <sup>st</sup> Century, in San Francisco.
May 2	Kirk Nahra will present “Beyond HIPAA: Further Privacy Concerns for Health Plans” at the Blue Cross Blue Shield Annual Lawyers Conference, in Orlando.
May 2	John Kamp will present “Washington Legal Update: Privacy on the Internet” to the Public Law Institute, in New York City.
May 3-4	Several WRF attorneys will make presentations at the conference on E-Commerce and Privacy for the “Old Economy” co-hosted by <i>Privacy In Focus</i> and Mealey Publications, in Philadelphia.
May 6	Kirk Nahra will speak on “The Top Twelve HIPAA Privacy Issues for Health Plans” before the American Association of Health Plans’ Managed Care Law Conference, in San Francisco.
May 10	Meredith Fuchs will participate in a panel discussion on “Regulatory Expectations of Privacy” at the Futures Industry Association Law & Compliance Division’s 23 <sup>rd</sup> Annual Workshop, in Baltimore.
June 18	Kirk Nahra will present “Beyond HIPAA: Developing an Integrated Privacy Program for Health Plans” at the Annual Meeting of the American Health Lawyers Association, in Orlando.
July 18	Tom Brunner will speak on “E-Commerce & Privacy” at the AEGIS E-Commerce Conference, in Chicago.

### **Contributors**

William B. Baker.....	202.719.7255.....	wbaker@wrf.co
Thomas W. Brunner.....	202.719.7225.....	tbrunner@wrf.cc
Kathryn Bucher.....	202.719.7530.....	kbucher@wrf.cc
Meredith Fuchs.....	202.719.3142.....	mfuchs@wrf.cc
John F. Kamp.....	202.719.7216.....	jkamp@wrf.cc
Andrew S. Krulwich.....	202.719.7003.....	akrulwic@wrf.cc

***Wiley, Rein & Fielding***

Marcus E. Maher.....202.719.4849.....mmaher@wrf.co  
Bruce L. McDonald.....202.719.7014.....bmcdonal@wrf.cc  
Kirk J. Nahra.....202.719.7335.....knahra@wrf.cc  
Dorthula Powell-Woodson.....202.719.7150.....dpowell-woodson@wrf.co  
John B. Reynolds, III.....202.719.7342.....jreynold@wrf.cc  
R. Michael Senkowski.....202.719.7249.....mike\_senkowski@wrf.cc  
Amy E. Worlton.....202.719.7458.....aworlton@wrf.cc