October 30, 2001 No. 16

Safe Harbor or Stormy Waters?
Living with the EU Data Protection Directive

by Aaron Lukas

Executive Summary

On July 1, 2001, the European Commission was scheduled to complete a one-year review of how well non-European companies were complying with the European Union's Directive on Data Protection. More important, that date was also supposed to mark the end of an informal standstill on enforcement of the directive's restrictions on cross-border data flows. Both the report and the end of the enforcement moratorium have been postponed, but for how long is uncertain.

The EU directive is designed to regulate the transfer and use of personal data about European citizens. One facet of that regulation is a prohibition on the transmission of personal data to countries outside Europe that lack "adequate" data protection laws. If strictly enforced, that prohibition could harm businesses and consumers on both sides of the Atlantic.

The EU-U.S. Safe Harbor agreement seeks to bridge the gap between the top-down European data protection regime and the more decentralized U.S. approach. Although Safe Harbor is still in its infancy, its survival is already in doubt. Few companies have signed up. Meanwhile, the EU continues to develop model privacy contracts that may further undermine the usefulness of the Safe Harbor framework.

At best, Safe Harbor faces an uncertain future. The United States should recognize that Europe has the right to set its own privacy policies but not be pressured into copying the EU's unwise data protection model. Relying on technology and market incentives, rather than regulation, to protect privacy empowers individual consumers to make their own choices, encourages new business and innovation, and protects free speech. The United States should stick to that course regardless of what Europe does. At the same time, however, if European law is enforced in such a way as to put U.S. companies at an unfair disadvantage—which is entirely possible—the United States should not hesitate to defend its interests through the dispute resolution mechanism of the World Trade Organization.

Aaron Lukas is a trade policy analyst with the Cato Institute's Center for Trade Policy Studies.

CATO INSTITUTE

The survival of the Safe Harbor agreement is already in doubt.

Introduction

> The right to be left alone—the most comprehensive of rights and the right most valued by a free people.
>
> Justice Louis Brandeis,
> *Olmstead v. U.S.* (1928)

> Fear of serious injury cannot alone justify oppression of free speech and assembly.
>
> Justice Louis Brandeis,
> *Whitney v. California* (1927)

On July 1, 2001, the European Commission was scheduled to complete a one-year review of how well non-European companies were complying with the European Union's Directive on Data Protection. More important, that date was also supposed to mark the end of an informal standstill on enforcement of the directive's restrictions on cross-border data flows. Both the report and the end of the enforcement moratorium have been postponed, but for how long is uncertain.

The Directive on Data Protection has been in force since October 25, 1998.[1] The law is designed to regulate the transfer and use of personal data—information that can be linked to a specific individual—on European citizens. In addition to harmonizing the data protection laws of EU member nations, which was the legislation's primary stated goal, the directive also prohibits the transmission of personal data to countries outside Europe that lack "adequate" data protection laws. Thus, extra-EU transfers of people's names, addresses, birthdays, or buying habits can all be blocked under the directive. Information that is not traceable to particular individuals, such as aggregated statistical data, is generally not subject to the export ban.

The directive's restrictions on international data flows have greatly concerned business leaders and public officials in Europe's major trading partners, most notably the United States. American businesses are world leaders in electronic commerce. They routinely collect and share various types of personal information, both domestically and in transactions involving customers and business partners in Europe. The disruption of such data flows would harm businesses and consumers on both sides of the Atlantic.

Unlike the EU, the United States does not have a centralized regulatory structure to govern the use and transmission of personally identifiable information. That fact led many European officials to speculate early on that the United States would not provide adequate protection of data on European citizens. Seeking to head off a potentially serious trade dispute, the U.S. Department of Commerce began earnest negotiations, led by Under Secretary David L. Aaron, with the European Commission in 1997. The intent of those negotiations was to bridge the gap between the European top-down legislative model of data protection and the more market-based approach, coupled with some sector-specific regulations, favored by the Americans.[2]

The negotiators finally unveiled the EU-U.S. Safe Harbor agreement in the summer of 2000, and after some initial hesitation, the agreement was approved by the European Union. Under the terms of the agreement, companies and organizations on a Safe Harbor list maintained by the U.S. Department of Commerce are automatically assumed to provide adequate data protection, as defined by the directive, and will not have business operations interrupted or face prosecution by European authorities.

The Safe Harbor agreement is barely a year old, but its survival is already in doubt. Fewer than 50 companies have so far chosen to be placed on the Safe Harbor list, possibly because prosecutions under the directive have been exceedingly rare. (Only two of those companies—Microsoft and Hewlett-Packard—engage in any significant business-to-consumer commerce.) Moreover, the European Union is currently developing model contracts that U.S. businesses can use to commit themselves to obeying European data laws on a case-by-case basis, which may further undermine the usefulness of the Safe Harbor frame-

work. This paper offers an early assessment of the agreement and speculates on the future of U.S.-EU privacy conflicts, as well as how a proliferation of national privacy laws may affect international trade more generally.

A Brief History of International Data Regulation

Standardized national rules for the processing and transmission of personally identifiable information, often known as fair information principles, were first proposed by the U.S. Department of Health, Education and Welfare in 1973.[3] Then-secretary of HEW Elliot L. Richardson had appointed an Advisory Committee on Automated Personal Data Systems a year earlier to explore the impact of computerized record keeping on individuals. The committee's report formed the basis for much of the subsequent law related to information collection, including the U.S. Privacy Act of 1974,[4] which safeguards against the misuse of personal records, primarily by federal agencies. In brief, the act allows U.S. citizens to learn how records are collected, maintained, used, and disseminated by the federal government. The act also permits individuals to gain access to most personal information about them maintained by federal agencies and to seek correction of any inaccurate, incomplete, or irrelevant data.

In 1980 the Organization for Economic Cooperation and Development issued a set of guidelines concerning the privacy of personal records. Those guidelines incorporated many of the recommendations from the 1973 HEW report. Those guidelines provide a model for most current international agreements, national laws, and private codes of conduct. The OECD guidelines have as key principles

- collection limitation,
- data quality,
- purpose specification,
- use limitation,
- security safeguards,
- openness,
- individual participation, and
- accountability.[5]

Taken together, the OECD principles require that as little personal information as possible be collected and that such information be used only for the purpose for which it was originally collected unless prior notice is given. People should be notified about what information about them is being collected, why the information is necessary, and who will have access to it. Individuals should be able to access information about themselves and have it corrected or deleted if necessary. The OECD principles stop just short of saying that information cannot be transferred to third parties without the explicit consent of the data subjects.

Another notable milestone in the codification of fair information principles was the United Nations' publication of its nonbinding "Guidelines for the Regulation of Computerized Personal Data Files."[6] Adopted by the General Assembly in December 1990, the guidelines—intended for use by national legislatures—essentially restated the OECD fair information principles with the addition of a troublesome Principle of Nondiscrimination, which says: "Data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled." The wording "data likely to give rise to" is so broad as to allow prohibition of practically all data collection. And as is often the case with UN guidelines, governments were given wide latitude to excuse themselves from the suggested data regulations.

Although national data laws originated in Washington, D.C., such laws have proliferated much faster elsewhere. Indeed, there continues to be a general consensus in the United States that market incentives and new technologies will be largely sufficient to protect privacy and that any new regulations should be as unobtrusive as possible. Put differently, if consumers desire that the information they disclose be used only for limited purposes, businesses will compete with each other to attract customers

Unlike the EU, the United States does not have a centralized regulatory structure to govern the use and transmission of personally identifiable information.

by giving them what they want. That approach is often called "market regulation," and it can lead to some interesting privacy-enhancing innovations, a few of which will be discussed later in this paper.

By contrast, Europe early on took a more aggressive, government-centered approach to regulating the communication of personal information. The first European data protection laws at the subnational level were passed by the German state of Hesse in 1970. Another major milestone occurred in 1981, when the Council of Europe incorporated the OECD principles into a treaty that was widely adopted by EU member governments. Known as the Council of Europe Data Protection Convention (Convention 108), the document formed the basis for many national data protection laws that were subsequently enacted throughout Europe.[7] Article 1 of Convention 108 concisely articulates the European justification for regulating personal data: "The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his *rights and fundamental freedoms*, and in particular his *right to privacy*, with regard to automatic processing of personal data relating to him."[8]

So from the very beginning, the right to control what others say about you was the basic assumption that underpinned privacy laws in Europe. The ownership of information about oneself is, in the dominant view of European elites, a self-evident human right that must be guarded by the state. As David Smith, assistant information commissioner for the United Kingdom, recently noted in testimony before the U.S. House of Representatives: "The human rights approach to Data Protection is clear. It is founded in the right to respect for one's private life."[9]

From the beginning, the right to control what others say about you was the basic assumption that underpinned privacy laws in Europe.

By the early 1990s, many EU member states had adopted national data protection laws. But despite a consensus on the need to regulate the communication of personal information in Europe, it was becoming apparent that the different legal standards adopted by the various countries were causing problems. Specifically, data transfers were sometimes blocked or subjected to nonuniform safeguards between countries. France, for example, threatened in the late 1980s to ban transfers of personal information by Fiat's French subsidiary to its parent company in Italy—a country that had no data protection laws at the time. Data regulation was, in short, becoming a barrier to trade within Europe.

Because of such intra-European disputes, the European Commission drafted the Directive on Data Protection, intended to harmonize the laws of the member states. The directive established minimum standards for the processing and use of personal data, not only to ensure that the member states protect the "fundamental right" to privacy, but also to prevent member states from engaging in intra-European trade protectionism by restricting the free flow of personal data under the guise of protecting privacy. As Article 1 of the directive states, "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection [of the right to privacy with respect to the processing of personal data]."[10]

For the directive to obtain the force of law throughout Europe, it needed to be adopted by the national legislature of each EU member. But because no two countries would be using precisely the same language—both literally and figuratively—implementation of the directive would not be uniform across countries. To smooth out differences, a European-level advisory body made up of the national data protection officials and a representative of the European Commission (the Article 29 working party) was established to coordinate implementation and advise the commission, which could then take additional action as needed. Thus, the directive authorized an ongoing, supranational regulatory role for the commission in an area that had formerly been entirely the province of national law. That was only the first jurisdictional impact of the directive.

In 1995 the directive was formally adopted by the Council of Ministers of the European Union. A deadline of October 1998 was set for the formal implementation of the directive by each member state. Despite the deadline, several EU

member states, including France and Germany, have yet to adopt legislation to implement the directive (although those countries already have similar data protection laws in place).

The Flawed European Data Directive

The directive applies to just about all "processing" of personal data.[11] It grants data subjects—people about whom information is collected—most of the rights suggested by the OECD. In practice, that means that data subjects have the right of access to personal data, the right to know what data are being collected and for what purpose, the right to know the identities of all parties that will have access to the data, the right to have inaccurate data corrected, the right to recourse in the event of unlawful processing, and the right to withhold permission to use data in certain circumstances (for example, individuals have the right to opt out, without charge, from being sent direct marketing material). Governments are exempted from most of the requirements of the directive, as are "natural person[s] in the course of a personal or purely household activity."[12]

The rights conferred on data subjects under the directive are difficult to enforce in a world where countries do not restrict the uses of personal information to the same degree. Once data leave the European Union, there is no way for its member governments to restrict the number of parties that gain access to the data or what those parties do with the information. The global free flow of data thus undermines the ability of the directive to control information about European citizens. Article 25 of the directive attempts to deal with this problem by restricting the transfer of information from the European Union to countries that fail to meet Europe's standards for adequate data protection. It is the Article 25 restrictions that most concern Europe's trading partners.

The question of exactly what constitutes "adequate" protection is key. The directive goes far beyond any U.S. data protection laws, especially in its provision for opting out of lawful data processing activities, such as marketing. Although many companies in the United States voluntarily allow their customers to opt out of receiving marketing information—and the Direct Marketing Association maintains a master list of people who prefer not to receive any product pitches at all—such "freedom from advertising" is not guaranteed by law.[13]

Such marketing techniques are not only permissible in the United States, they are common. For example, an online sporting goods store based in Arkansas may observe that some of its customers have an interest in fishing. Naturally, the store wants to cater to the customers' tastes by making them aware of all the fishing-related products it carries. The store bases its judgment about customers on several factors: its record of tackle sales to various individuals, the amount of time people spend browsing the rods and reels section of the company's Web site, and the fact that some customers may subscribe to *Field and Stream* magazine. Assuming that such information was not obtained through force or fraud, and that no contractual obligation not to share information was violated, there is no obvious reason to assign ownership rights to that information to the data subject rather than to the party or parties that collected it. Despite the proliferation of data protection rules in the United States, such marketing practices remain legal and are widely accepted.

Another difference between the United States and Europe is the legal protection accorded speech. The "rights" granted to data subjects under the directive translate into restrictions on people who want to communicate personal information. That result runs contrary to deeply held American convictions about free speech and the right of individuals to express themselves, protected under the First Amendment to the U.S. Constitution. Thus, laws intended to curtail the communication of factual information that has been legally obtained, even when that information concerns a specific individual, have been tightly restricted as a violation of free speech. So, if in calling for "adequate" data protection the directive means that the United States must mimic Europe's top-down approach to privacy regulation at the expense of free speech, serious dis-

The "rights" granted to data subjects under the directive translate into restrictions on people who want to communicate personal information.

putes are coming. As the quotes from Louis Brandeis—an early American supporter of the "right" to privacy—at the beginning of this paper illustrate, the tension between free speech and the desire of individuals to be left alone has greatly influenced the course of personal data regulation in the United States.

In addition to restricting speech, the European approach to regulating personal information is costly. The expense of offering consumers access to all data that have been collected about them, for example, especially information that is neither sensitive nor critical, would require companies to make large investments in new hardware, software, and personnel. Those costs are passed on to consumers in the form of higher prices for goods and services. Although it is impossible to gauge the full price of such policies, several new studies have attempted to make ballpark estimates of the losses. One such study, conducted by Ernst & Young for the Financial Services Coordinating Council, estimated that at least $16 billion worth of financial services would be lost if EU privacy standards were adopted for financial services in the United States. The study also predicted that bank and insurance customers would be forced to spend an additional 305 million hours annually on their personal finances.[14] Another recent report, this one published by the American Enterprise Institute–Brookings Institution Joint Center for Regulatory Studies, concluded that it would initially cost U.S. firms up to $36 billion to comply with across-the-board European-style privacy standards.[15]

In addition to restricting speech, the European approach to regulating personal information is costly.

Another, less obvious, cost of the EU-style privacy regulation may be an end to free content on the Internet. A large number of Web sites support themselves by collecting information about their visitors and then selling that information to advertisers who want to precisely target potential customers. A free online fashion magazine, for example, may collect contact information from its readers as a condition of accessing its articles. The collected names and addresses are then sold to a large clothing retailer. The retailer sends catalogs to people on the list, hoping that people who read online fashion magazines will have an interest in buying clothes. Selling the information about its readers allows the online magazine to publish without charging a fee.

Such exchanges of information make much of the free content on the Internet viable. If the privacy standards embodied in the directive are imposed on U.S. companies via the Article 25 sanctions, those companies could be required to offer their services without being able to sell the information they collect. That would make many sites unprofitable, and they would either shut down or be forced to charge for content.[16]

Because of those financial and legal factors, the government's role in regulating data exchange in the United States has, with some notable exceptions, been largely limited to adjudicating disputes in the courts and prosecuting cases of outright fraud by businesses. Given the rapid growth of electronic commerce in America relative to other areas of the world, the market-based approach to regulating personal data has arguably been a success.

Of course, material prosperity, and even free speech, is not valued equally around the world. It has long been observed that Europeans weigh the competing values of free expression and privacy differently than do most Americans. That difference is often attributed to the European experience with totalitarianism and the manner in which personal information, gathered from both official and private sources, has been misused by governments in the past. (The fact that governments are exempt from most of the directive is a contradiction that proponents of this explanation seem to have missed.) In addition, many Europeans seem to be more culturally suspicious of corporations and "big business" than are their cousins across the Atlantic. The directive, while hostile to free speech (and effective marketing), obviously meets a European policy preference for restrictions on how people communicate about one another. Americans may question the merit of that preference, but we cannot write European laws.

Unfortunately, the fact that the directive may be popular among Europeans does not make it a well-crafted document or easy to obey.

Though the law lays out general principles of data protection, those principles are often so vague as to provide virtually no guidance about how to comply with them in the real world. The principles are also, of necessity, riddled with exemptions that can be interpreted either broadly or narrowly. The various possible readings can lead to wildly different prescriptions about how businesses should behave. The shortcomings of the directive have been extensively documented elsewhere and so will not be covered in detail here.[17] One example should suffice to illustrate the nature of the problem facing foreign persons and businesses that are involved with information transfers to and from Europe.

Consider the case of a U.S. company that manufactures, installs, and services photocopiers for European customers. In order to avoid costly unnecessary service visits, the company provides technical support via telephone and e-mail to handle problems that do not require a technician. The call center and Web site are physically located in the United States. When a call or e-mail comes in, technical support personnel need to view the account information and service record of the customer who is experiencing difficulties.

If that customer is in Europe, the directive governs the transfer of any records. In general, Article 25 would prohibit the transfer of such information from the European sales office to the U.S. call center. The transfer might be allowed, however, under one of the exceptions listed in Article 26 of the directive. One option might be for the customer to give permission to transfer service records at the outset of the call (Article 26(1)(a)). But if the person making the call was not the data subject but a part-time employee working for a small businessman operating out of his home, the copier company could not be sure that it was in compliance with the law. Moreover, if the company did not provide technical support to callers who refused to consent to information transfers, European data authorities might conclude that consent was not voluntary. A second option might be for the business to claim that the transfer of records outside of Europe is "necessary for the performance of a contract in the interest of the data subject" (Article 26(1)(b)). In that case, the business must worry about whether all the information transferred is truly "necessary" to providing the service. What if the information is merely "useful" but not strictly "necessary"? The directive provides no guidance on such matters.

Because of its lack of clarity, the directive leaves EU privacy officials with enormous discretion in enforcing it. This arrangement is perhaps convenient for European lawmakers, who are able to claim credit for "protecting privacy" without being held accountable for the directive's costs. But such an approach is a nightmare for the individuals and organizations that are faced with the uncertainty of complying with rules that no one fully understands and that have, in a sense, yet to be written. Of course, the inefficiencies and lost economic opportunities generated by the directive may be a cost that Europeans are willing to bear. The question that U.S. policymakers are still struggling to answer is this: does the directive go too far in imposing EU law on the international economy?

Extraterritorial, Protectionist, or Both?

The directive has potentially profound extraterritorial effects, as would any national legislation that sought to regulate information that crosses borders. Specifically, Article 25 of the directive authorizes EU authorities to halt information transfers to countries that do not meet European privacy standards. Critics argue that such restrictions are imposing, intentionally or not, Europe's privacy preferences on other countries. House Energy and Commerce Committee chairman Billy Tauzin (R-La.), for instance, has charged the European Union with attempting to force a "de facto privacy standard on the world."[18] Even members of Congress sympathetic to the directive tacitly concede Tauzin's point but counter that extraterritoriality is not a problem in this case and that the United States would be wise to follow Europe's lead.[19]

The extraterritorial nature of the directive has led to comparisons with Washington's Cuban Liberty and Democratic Solidarity (or Helms-

Because of its lack of clarity, the directive leaves EU privacy officials with enormous discretion in enforcing it.

An important question is whether the directive is consistent with the commitments made by EU member states when they joined the World Trade Organization.

Burton) Act of 1996, which grants U.S. citizens whose property was expropriated by Castro the right to sue in U.S. courts foreign companies and citizens "trafficking" in that property (Title III).[20] That right—not granted to U.S. citizens who may have lost property in other countries—is problematic because it essentially extends U.S. jurisdiction to the results of events that occurred on foreign territory. European governments have been some of the strongest opponents of the U.S. effort to apply its domestic laws beyond its borders. If the United States is wrong to impose its will on European companies who defy U.S. law, critics ask, should not Europe be held to the same standard?

But the analogy may not be entirely appropriate. Extraterritorial *effects* of a law are not necessarily the same thing as extraterritorial *application*. In the case of Helms-Burton, the primary purpose of the law is to hold liable foreign companies that "traffic" in Cuban assets that the U.S. government considers stolen. No connection to the United States or a U.S. entity need be established before the foreign company runs afoul of U.S. law. And once the provisions of Helms-Burton are violated, not only can the foreign company be sued in U.S. court, but the United States may apply trade sanctions against the company's country of residence. Helms-Burton is an example of the extraterritorial *application* of U.S. law because it seeks to directly control behavior outside the United States.

The directive, however, is focused mostly on the behavior of European companies—or European affiliates of U.S. companies—operating within Europe and undeniably falling within the EU's jurisdiction. The directive forbids those companies to transfer personal data to non-EU countries that have what EU privacy officials determine to be inadequate rules regulating how data can be used. That transfer restriction will indeed have an impact on non-EU businesses, but that is not the same as saying that such businesses are being unfairly subjected to European law. In this case, the *effect* of the directive is extraterritorial; its application may not be. This distinction does not necessarily mean that the directive is good policy, but it does distinguish it from truly extraterritorial laws like Helms-Burton.

Is the Directive Illegal under WTO rules?

An important question is whether the directive is consistent with the commitments made by EU member states when they joined the World Trade Organization. The WTO—and its constituting document, the General Agreement on Tariffs and Trade—commits signatories to two core principles in matters of trade: most favored nation and national treatment. The most favored nation principle means that a country will not discriminate among its trading partners. In other words, the highest level of market openness offered to any one country, the "most favored nation," must be offered to all countries that are party to the GATT. The national treatment principle means that once a country grants market access to a foreign company, that company will be treated as if it is a domestic firm. Thus, national treatment would forbid a GATT signatory from applying different emissions standards to imported automobiles, for instance, than are applied to those built domestically.

The directive may violate either or both of those trade commitments. Consider the example of two companies that provide data processing services, one located inside Europe and the other based in California. Assume that the companies have identical data protection policies and that those policies conform to the requirements of the directive. Because the company in California is located in a country that relies more on market competition than on government regulation to protect personal data, potential buyers of its data processing services within Europe face the possibility of legal sanction under the directive if they decide to do business with the U.S.-based firm. The clear effect of the directive in this case would be to give a competitive advantage to the European provider of data processing services, despite the fact that the two companies follow identical data protection procedures. In other words, the directive may condition access to the European market on the legal regime in foreign countries. That would be akin to a rule saying that cars built in Detroit could not be imported into Europe because Michigan has looser air quality rules than Brussels prefers, even when the

cars in question meet EU emissions standards. On the surface at least, that would seem to be a violation of national treatment.

There is also tremendous room for discrimination *among* countries under the directive. If Canada is deemed to provide adequate protection for personal data, for example, while the United States is not, U.S. trade officials might be able to make a good case that trade barriers are being applied arbitrarily, in violation of the most favored nation principle. After all, laws do not have equal results, and it is certainly debatable whether the European top-down approach to regulating the use of personal information actually works as advertised. A recent study by Consumers International found that Web sites based in the European Union are no more—and often less—likely than are others to meet the directive's privacy standards. "Despite tight EU legislation in this area," the report states, "researchers did not find that sites based in the EU gave better information or a higher degree of choice to their users than sites based in the U.S. Indeed, US-based sites tended to set the standard for decent privacy policies."[21] Anecdotal support for the report's conclusion is not difficult to find. In an informal survey of U.K.-based Web sites conducted by the author of this paper, 10 Web sites that failed to adhere to the directive's core requirements of notice and choice were located in less than 15 minutes.[22] Ironically, threats from Europe and public pressure at home have led most U.S. companies to post privacy policies on their Web sites, while few EU companies feel the need to do so because they are already bound by broad privacy laws. The result may be that consumers are better informed about how data on them are used by American companies than by European companies, the opposite of what the directive was intended to accomplish.

Obviously, there are discrepancies between the promise and the reality of data protection in Europe. It seems arbitrary to ban businesses from competing in the European market for information processing on the sole basis of the *manner* in which personal information is safeguarded in their home countries, even though the overall level of protection may be greater than that which exists in Europe. It would be akin to a rule saying that hair dryers could not be imported from the United States, even though they were not dangerous to consumers, because U.S. manufacturers are regulated by Underwriters Laboratories, a private entity, rather than by the federal government. How is such a distinction meaningful if the result is quality hair dryers? It is doubtful that such a rule would survive a WTO challenge.

WTO Precedent: Shrimp-Turtle, Tuna-Dolphin

Consider the precedent of the WTO's decision against the United States in the well-known "shrimp-turtle" case. The dispute surrounded a U.S. ban on imports of shrimp from countries that did not mandate turtle excluder devices—trap doors in shrimp nets that allow sea turtles that are inadvertently caught to escape unharmed. Ostensibly, the purpose of the U.S. rule was to protect sea turtles, not to protect its domestic shrimp industry, though in matters of trade it is perhaps impossible to fully divorce intentions from outcomes.

Several countries, including major shrimp-exporting nations like India and Thailand, challenged the U.S. rule in the WTO on the grounds that the U.S. law was (a) not justified under the allowable exceptions to WTO rules against trade restrictions and (b) being applied in a discriminatory manner. The United States lost both the original case and the appeal, albeit for different reasons. The original panel report found that the United States' shrimp ban constituted unjustifiable discrimination against countries where the same conditions prevail. In addition, that discrimination was not held to fall under the exceptions listed under Article XX of the GATT, which allow trade barriers that are "necessary to protect human, animal or plant life or health" or related to "the conservation of exhaustible natural resources, if such measures are made effective in conjunction with restrictions on domestic production."

In its report, the dispute panel wrote, "In our view, if an interpretation of [Article XX] were to be followed which would allow a Member to adopt measures conditioning access to its market for a given product upon the adoption by the

Consumers are better informed about how data on them are used by American companies than by European companies, the opposite of what the directive was intended to accomplish.

exporting Members of certain policies . . . GATT 1994 and the WTO could no longer serve as a multilateral framework for trade among Members as security and predictability of trade relations under those agreements would be threatened."[23] The panel further found that the U.S. import restriction was "a measure conditioning access to the U.S. market for a given product on the adoption by exporting Members of conservation policies that the United States considers to be comparable to its own in terms of regulatory programmes and incidental taking"[24] and so "constitutes unjustifiable discrimination between countries where the same conditions prevail and thus is not within the scope of measures permitted under [Article XX]."[25]

Although the Appellate Body determined that the United States was justified under Article XX in trying to protect sea turtles, it agreed with the panel that the United States was engaging in arbitrary discrimination and unnecessary trade restriction. "[The U.S. law], in its application," the appellate report said, "is, in effect, an economic embargo which requires *all other exporting Members*, if they wish to exercise their GATT rights, to adopt *essentially* the *same* policy (together with approved enforcement program) as that applied to and enforced on, United Sates domestic shrimp trawlers."[26]

Certainly, much of the reasoning, both of the original panel and of the Appellate Body, could be applied to a future WTO case over Europe's restrictions on data transfers. Although Europe would likely argue that the directive is necessary to protect the fundamental human right to privacy, and thus exempt from WTO restrictions on barriers to trade, it can reasonably be concluded that the EU is applying those laws in a manner that discriminates "between countries where the same conditions prevail." The case would ultimately turn on whether the directive was actually being applied in such a manner as to constitute abuse or misuse of one of the exceptions to basic GATT principles. Although it is probably too soon to make this judgment, the potential clearly exists.

It may also be instructive to look at the 1991 "tuna-dolphin" dispute between the United States and Mexico that was adjudicated under the GATT.[27] The United States banned imports of Mexican tuna because Mexico had not taken steps to reduce the number of Eastern Pacific tropical dolphins killed each year in the course of tuna fishing. Mexico appealed the case to the GATT, where the dispute resolution panel ruled in favor of Mexico. The decision was based partly on the discriminatory manner in which the United States had implemented the measure and partly on GATT resistance to trade-restricting measures based primarily on the process of production.

The directive could certainly be indicted on those grounds. On what basis will countries be classified as providing "adequate" data protection? That question remains unanswered. Might not European officials make their findings of adequacy in a manner that discriminates among WTO members? And even if the directive is applied in an evenhanded manner, might not data protection laws be viewed as akin to the "production process" by which data services are provided?

Proliferating Protectionism

Finally, there is the question of the cumulative impact of the directive on international data flows over time. Its passage preceded, if not outright prompted, a proliferation of new national laws governing the acceptable uses of personally identifiable information in countries around the world. Since the directive became effective in 1998, new restrictions have been passed in Argentina, Australia, Canada, Chile, Paraguay, and other countries. The Safe Harbor agreement, which governs only data exchanges between the United States and Europe, is thus in one sense already inadequate for heading off potentially costly and disruptive international privacy disputes. It is also possible, however, that the agreement, if it is ultimately successful, can serve as a model arrangement for bridging the differences between nations with respect to privacy law.

Although it is almost certainly true that the directive was created for the purpose of protecting the privacy of individual European citizens, it is equally true that the law has the potential to become the tool of protectionist business interests. Consider again the field of data processing and warehousing. Many businesses find it more

Since the directive became effective in 1998, new restrictions have been passed in Argentina, Australia, Canada, Chile, Paraguay, and other countries.

affordable to contract out major information processing tasks than to do the job in-house. Similarly, it is often desirable, in terms of both cost and security, to store large amounts of data, such as customer purchase records, in a specialized off-site data warehouse. From a technological standpoint, it does not matter where a business chooses to have its information processed and stored; it only matters how well and how competitively the data processing firm can do the job. Many U.S.-based businesses are leaders in this area and process large amounts of information transferred from Europe.

Under the directive, however, European businesses seeking to contract out their data processing tasks have a strong incentive to avoid the uncertainty and potential liability of dealing with a firm located outside Europe. Conversely, for a data processing company in the United States, the incentive may be to withdraw from the European market altogether if the costs of compliance with the directive—say for retooling its software and hardware—are prohibitively high. Although most large companies would probably be able to cover the costs of compliance, some smaller firms would be likely to forsake the European market altogether if the directive were to be stringently enforced. Because the removal of American competition would benefit EU-based data processing firms, they have a strong incentive to pressure regulatory authorities to narrowly interpret the prohibitions on data transfers to third countries. If that happens, other countries will almost certainly follow suit, much as the developing world has copied the reckless use of antidumping and other trade "safeguard" laws by the United States in Europe in recent years.

The Safe Harbor Agreement

Because the rules governing personal data under the directive are more restrictive than those of the United States, and their potential impact on trade is significant, U.S. policymakers began to look for a way to mitigate the directive's negative effects even before the document was formally implemented. Of particular concern to U.S. businesses were Articles 25 and 26, which govern the transfer of data to any person or entity based outside the European Union. As noted earlier, Article 25 conditions data transfers outside of Europe on the "adequacy" of the privacy protections provided by the destination country. Article 26 lists the exceptions to that general rule.

In perhaps the most comprehensive assessment of the directive to date, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*, law professor Peter Swire and Brookings Institution economist Robert Litan sought early on to alert U.S. businesses to the possible impact of the new privacy rules on their data flows to and from Europe. "The big rule is that data can't be transferred to countries that lack 'adequate' protection," noted Swire (who was later appointed chief counselor for privacy in the Clinton White House). "The EU will not make a finding that the United States has adequate protection," he cautioned. "Nor has it said it is inadequate across the board. So all transfers to the United States are potentially at risk under the new law."[28] Swire and Litan dissected the directive and exposed a great deal of ambiguous language in the document. They also pointed out that many routine business practices could be considered illegal under the directive. The uncertainty that this would create for U.S. businesses engaged in data transfers from Europe, they concluded, was significant and could prove costly.

As uncertainty about the impact of the directive on U.S. businesses increased, it became evident that Washington needed to begin a dialogue with Brussels. A delegation headed by Under Secretary of Commerce David Aaron was dispatched in mid-1998 by the Clinton administration. The Aaron delegation proposed a "Safe Harbor" arrangement, whereby U.S. companies could comply with the directive by agreeing to abide by a list of privacy principles that both the U.S. government and the EU found acceptable. From the very beginning, the EU's Article 29 working party found fault with several aspects of the proposed U.S. scheme. Specifically, the working party emphasized the need for a more general right of "subject access" and for more stringent government monitoring

European businesses seeking to contract out their data processing tasks have a strong incentive to avoid the uncertainty and potential liability of dealing with a firm located outside Europe.

Once data leave the European Union, there is no way for its member governments to restrict its uses.

and enforcement mechanisms than the United States was willing to concede.[29] The United States argued that giving individuals access to all data held about them would be prohibitively expensive and that private organizations could be relied on to police privacy practices.

It would take two years of sometimes contentious talks—until the spring of 2000—before U.S. and European negotiators announced that they had bridged the differences between the conflicting approaches to regulating personal data.[30] The deal they had brokered, commonly known as the Safe Harbor agreement, included a list of information management practices to which U.S. companies must adhere in order to engage in the transfer of personal data from Europe. Safe Harbor made it possible for businesses to keep transferring information to and from Europe even if the United States were found to offer "inadequate" data protection under Article 25 of the directive. Hopes at the time were high. EU internal market commissioner Frits Bolkestein described the arrangement as providing "a framework within which personal data transferred to the U.S. will be better protected, while at the same time making transfers simpler for both EU and U.S. businesses."[31] U.S. negotiators were equally upbeat: "I'm more than optimistic that the Safe Harbor is going to work," said Charles Ludolph, deputy assistant secretary for Europe in the Department of Commerce's International Trade Administration. "We agreed with the European Union that this is an open-ended evolving process that is intended to allow the Safe Harbor to succeed."[32]

Companies that agree to abide by the Safe Harbor standards are certified by the U.S. Department of Commerce and listed on the Internet. Certifying to the Safe Harbor signals to EU data regulatory agencies that a company provides "adequate" privacy protection, as defined by the directive, and thus is eligible to receive data flows from Europe without obtaining other prior approval. In other words, Safe Harbor is intended to help U.S. companies "avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws."[33] In addition, claims of privacy violations brought by European citizens against U.S. businesses on the list will in most cases be heard in the United States.

The decision to meet Safe Harbor principles and self-certify with the Commerce Department is entirely voluntary on the part of U.S. businesses. In other words, the government does not audit domestic privacy practices under the agreement. Instead, a business must apply for Safe Harbor certification at which point it pledges, both in writing to the Commerce Department and publicly in its privacy policy statement, to abide by a specific set of seven information practices. Annual renewal is required to stay on the Safe Harbor list.

The seven Safe Harbor principles that a company must agree to follow are nearly identical to the OECD fair information principles discussed above:

1. Notice: Organizations must tell the data subject what information is being collected and how that information will be used, including the identities of any third parties that may receive the data. Contact information must also be provided for the purposes of taking complaints or questions.
2. Choice: Organizations must offer data subjects the opportunity to opt out of having information about them transferred to a third party or used for other purposes not directly related to the reason the information was initially collected. The data subject must affirmatively opt in before "sensitive" information, such as religious or political affiliation, before can be transferred or used for other than the purpose for which it was originally collected.
3. Onward Transfer: Organizations must apply principles 1 and 2 to all transfers of information to third parties. If the third party is acting as an agent for the organization that originally collected the information—by providing computer processing services, for example—information may be transferred if the third party (a) is also certified on the Safe Harbor list; (b) is subject to the directive (i.e., located in Europe); (c) has been found to offer "ade-

quate" data protection through some other means, such as contractual arrangement with a European privacy agency; or (d) signs a written agreement with the data holder requiring that the third party adhere to Safe Harbor principles before the information can be transmitted.

4. Access: Data subjects must have access to the information that an organization has collected about them and the ability to "correct, amend, or delete that information where it is inaccurate."[34] Exceptions are allowed for cases in which the burden or expense of providing access is "disproportionate to the risks to the individual's privacy in the case in question," or where the rights of some person other than the data subject would be violated.[35] Of course, depending on how that exception clause is interpreted, nearly all or no information about a person could be subject to the access requirement.
5. Security: Data holders must take "reasonable precautions" to ensure that information is not stolen, lost, misused, or altered.
6. Data Integrity: Data holders must take "reasonable steps" to make sure that the information they collect is accurate and relevant to the purposes for which they collect it.
7. Enforcement: There must be readily available independent recourse mechanisms to adjudicate and investigate individuals' complaints against data holders, and some form of compensation or damages must be available to individuals whose privacy is violated. In addition, there must be some independent assessment of how well an organization is living up to the commitments it made under Safe Harbor, and, if it is found wanting, there must be "sufficiently rigorous" sanctions applied in order to ensure compliance. Organizations that fail to comply with their Safe Harbor obligations must be decertified. The Commerce Department expects that most enforcement "will be carried out in the private sector."[36]

Enforcement Issues

Some of the most intractable disputes during the Safe Harbor negotiations reportedly surrounded the final Safe Harbor principle: the question of who will enforce compliance with the rules. EU negotiators expressed strong skepticism that the program could be effective without significant regulatory oversight by the U.S. government, while U.S. officials argued for more self-monitoring by the private sector. The U.S. position was that if the Safe Harbor agreement was to be a "bridge" between different approaches to managing personal data, and not simply a case of the United States' adopting European regulations in their totality, then some aspect of the U.S. self-regulatory system had to be preserved.

The agreement walks a fine line in this area: it does not necessarily grant new regulatory authority to the federal government of the United States, but it *does require* organizations that want to be certified to have in place a dispute resolution system and an independent means of verifying compliance with their privacy commitments. So far, it seems that private-sector compliance monitoring by organizations will fulfill this requirement. Ultimately, government-enforced compliance is still an option since the Federal Trade Commission retains its authority, under the rubric of protecting consumers from fraud, to punish organizations that violate their stated privacy principles. As the Commerce Department explains, "Where a company relies on self regulation in complying with the Safe Harbor principles, its failure to comply with such self regulation must be actionable under federal or state law prohibiting unfair and deceptive acts or it is not eligible to join the Safe Harbor."[37]

In addition, Europeans who believe that their privacy has been violated are eligible for relief through the U.S. court system. Indeed, the Commerce Department went to some lengths to reassure the EU that a failure to live up to Safe Harbor commitments can (but will not necessarily) result in monetary damages: "The relevant representation," the department wrote in a letter to the European Commission, "is the organization's public declaration that it will adhere to the safe harbor principles. Having made such a commitment, a conscious failure to abide by the principles could be grounds for a cause of action for misrepresentation

The self-regulation embodied in Safe Harbor is backed up by the force of government—through both regulatory agencies and the courts.

Broadly speaking, U.S. companies remain relatively unregulated in terms of how they may manage personal data.

by those who relied on the misrepresentation."[38] Thus, the self-regulation embodied in Safe Harbor is backed up by the force of government—through both regulatory agencies and the courts—but only generically, in the sense that no organization can legally engage in fraud or negligent misrepresentation of its privacy policies.

Broadly speaking, however, U.S. companies remain relatively unregulated in terms of how they may manage personal data. However, once an organization commits itself to abide by European privacy standards via Safe Harbor certification, its failure to comply with those standards becomes legally actionable. Indeed, the FTC already has statutory authority to seek administrative orders and civil penalties of up to $12,000 per day[39] against organizations that engage in fraud or misrepresentation. The European Union has also recognized the authority of the Department of Transportation to investigate privacy complaints under Title 49, U.S.C. sec. 41712. Not all businesses are pleased with this arrangement: "It's kind of a sobering thought, recognizing the fact that you're about to sign this certification that says that you're agreeing that the Federal Trade Commission can come in and investigate you," said Christopher W. Holmes, general counsel and director of human resources, Aeritas Inc., a mobile telecommunications provider.[40]

Despite the threat of government action, most of the day-to-day monitoring of compliance with Safe Harbor will be undertaken by private organizations, such as TRUSTe and the Better Business Bureau Online—two groups that specialize in certifying that businesses adhere to fair information practices.[41] First-tier sanctions against violators will likely be private as well. Persistent violators of Safe Harbor commitments will be removed from the certification list and will, presumably, be ineligible to receive personal data transfers from Europe. How stringently that provision will be enforced, however, depends largely on the nature of the business in question.

Size Does Matter

It is still unclear whether or not the directive applies to U.S. companies that lack a physical presence in Europe. Many Europeans believe it does; Americans disagree. "Anyone who is collecting personal data within the EU has to abide by the directive. . . . [He doesn't] need to have a physical office," says Alexander Dix, data protection commissioner for the German state of Brandenburg. Dix and others point to a provision in the directive that says the law will apply to anyone "making use of equipment" within Europe for transmitting personal information.[42] Negotiators failed to deal with the issue during the Safe Harbor talks, leaving little incentive for U.S. Web companies to sign on to Safe Harbor or take any other major steps to comply with the directive because they believe it does not apply to them, and even if it does, enforcement will be impossible. "People comply with laws because they think they will get caught," notes Gary Clayton, chief executive of Privacy Council, a Dallas firm that provides advice on corporate privacy issues. "The reality is a lot of Web companies are going to make a decision. . . . 'What are they going to do to me?'"[43]

It is indeed difficult to imagine how EU privacy officials could enforce the directive against foreign Web sites run by companies that have no physical presence in Europe. Even a cursory search of the Internet reveals thousands of small online retailers, such as Toad Suck Creations of Imbler, Oregon, that collect detailed personal data without any notice of how the data will be used, whether they will be sold or shared, or an opportunity to opt out.[44] Toad Suck Creations, like many other businesses on the Internet, does not follow any of the fair information principles that the directive seeks to impose. There is nothing wrong with that; European shoppers can choose to patronize such online stores or not on the basis of their own criteria. When they do so, however, they will be violating European law. Because these virtual retailers lack offices or assets in Europe, there is little that EU authorities can do to stop these transactions short of shutting down, or severely limiting, Internet access in Europe. Neither move is particularly plausible.

Thus, there is likely to be a wide discrepancy in the way the directive is enforced against information-transferring entities of different sizes. Large businesses such as the online bookseller Amazon.com are relatively easy to police and pun-

ish for violations of the directive. But large multinational businesses are already extremely likely to protect information about their customers and to disclose how that information will be used. A survey by the Federal Trade Commission last year found that 88 percent of all Web sites and 100 percent of the most popular Web sites in the United States disclose what information they collect and how that information is used.[45] Many of those companies have offices in Europe and are unequivocally subject to EU law. Smaller Web sites based outside Europe are far less likely to post, or even have, a privacy policy.

There is also the question of the legal status of personal Web pages under the directive. Personal pages often list personal data such as names, birthdays, addresses, and photographs. Are such Web sites "exporting" that information? After all, it can be viewed anywhere in the world, even in countries that lack privacy laws. That would seem to violate the Article 25 prohibition on the transfer of personal information to countries that lack adequate protection. If, for example, a high school student decides to create a site that contains the names, ages, and even pictures of her friends, is she in violation of the directive? Strictly speaking, the answer seems to be yes, since there is no Article 26 exception that would apply in that case unless one assumes that, simply by virtue of their relationship, the friends in question have granted tacit consent to publish personal information about them.

A widespread crackdown on personal Web pages under the directive is exceedingly unlikely. For one thing, many of those pages are difficult to locate unless you know exactly what to look for. Many of those pages are not indexed in search engines, and even when they are, literally millions of pages would have to be screened in order to root out violations. European privacy offices do not have the resources to do that even if they wanted to. And government monitoring of personal Web sites would rapidly undermine the public legitimacy that the directive seems to enjoy.

Exceptions to the Rules

The directive is a confusing document that sometimes seems contradictory. If vigorously enforced, the core principles of the directive—notice and choice—would completely disrupt life in Europe since the ability to freely communicate the details of one another's lives is something that all people take for granted on a personal level. If we truly "own" information about ourselves, then others should need our permission before speaking about us. Gossip, journalism, and indeed everyday conversation would become impossible.

The directive would not be even marginally functional without numerous exceptions to its core rules. In general, Article 26 offers the following exemptions, which, when one or more apply, would allow for the transfer of data out of Europe to a country that lacks "adequate" data protection rules.

- The data subject has given unambiguous consent to the transfer.
- The transfer is necessary for the performance of a contact in the interest of the data subject.
- The transfer is justifiable on "important public interest grounds" or for the exercise or defense of legal claims.
- The transfer is necessary to protect the "vital interests" of the data subject.
- The transfer is made from an open public data source.

Unfortunately, those derogations do not necessarily make it easier for U.S. businesses to comply. For example, it is unclear whether data that are allowed out of Europe under Article 26 exceptions are still governed by the directive. Consider the example of a U.S. clothing retailer that transfers data from an affiliate in Europe in order to fulfill its orders. Arguably, the transfer of information is "necessary for conclusion or performance of a contract concluded in the interest of the data subject and the controller [of the data]," in which case a transfer would be allowed even if the U.S. company were not a member of Safe Harbor.[46] Now assume that the retailer wants to transfer the information to yet another country for payment processing. Are data that have left the European Union under one of the Article 26

If, for example, a high school student decides to create a site that contains the names, ages, and even pictures of her friends, is she in violation of the directive?

exceptions still subject to the transfer restrictions in Article 25? The answer to that question is not clear; it could, however, have a tremendous impact on the way U.S. firms do business with Europe.

It should also be remembered that the directive has many exceptions covering uses of information inside Europe. For example, data may be kept for personal and household use like a phone book. Churches, trade unions, social clubs, and other nonprofit groups are permitted to keep even "sensitive" information, such as political or religious affiliation, about their members. Businesses may collect information without permission if it is in the "vital interest" of the data subject. Governments are permitted, though not required, to exempt journalists from the directive when free speech is judged to outweigh privacy interests. Given the large number of exceptions, the "fundamental right to privacy" turns out not to be quite so fundamental after all.

Privacy Rights: Do You "Own" What People Know about You?

Do businesspeople have the right to freely communicate information they obtain about their customers in the course of commerce?

Before assessing the impact of the directive and the effectiveness of the Safe Harbor agreement, it is useful to briefly examine the fundamental nature of "privacy rights." In practical terms, this boils down to the following question: should private companies be prohibited from keeping information about their customers' buying habits and sharing that information with other businesses? Or put differently, do businesspeople have the right to freely communicate information they obtain about their customers in the course of commerce? If, as is often asserted, consumers somehow own information about themselves, then presumably the answer to the preceding questions is no, and individuals have the right to control how information about them is circulated.

The notion that privacy is something to which individuals have an inherent right goes largely unquestioned in contemporary discussions about protecting personal information. In his prescient 1967 book, *Privacy and Freedom*, Columbia University legal scholar Alan Westin argued, "Privacy is the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others."[47] Privacy, Westin asserted, is not tied merely to the right to control one's own person and physical property—for example, by hanging curtains on an open window or kicking trespassers off private land. Instead, privacy is a freestanding claim of ownership of the intangible and dispersed knowledge that others have about you. Privacy is "ownership" of information. Such ideas, though not unique, were not commonly held three decades ago.

Today the notion of an independent "right to privacy" is staunchly defended by a new breed of professional "privacy advocates" and often drives policy debates in Washington. "Privacy is a fundamental human right recognized in most major international treaties and agreements on human rights," writes David Banisar, deputy director of Privacy International. "Nearly every country in the world recognizes privacy in their constitution, either explicitly or implicitly though court decisions. Most recently drafted constitutions include specific rights to access and control personal information."[48] Clearly, the European Data Directive adheres to that view. Its means of protecting personal data has been to "propertize" it—to create a right for the data subject to control how much and to whom information about him is allowed to flow. Indeed, the notion that a person has the right to control information about himself is at the core of EU data protection law, which is intended to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[49]

Property and Privacy

Privacy and property are in fact connected, but not in the way that the authors of the directive assume. Knowledge held by others is not property in the sense that a car or a house is property. If it were, then to know something about another person would reduce his well-

being in the same way that stealing his car would. To know that "John has a blue Volvo," after seeing him drive down the street, and even to tell a friend about the existence of John's car, does not unjustly injure John, even if John prefers that his preference in cars remain a secret.

Nevertheless, the natural right to own property does protect individuals from invasions of their privacy by placing limits on how others may obtain information about them. Privacy is in this sense a restriction on the ability of others, including the state, to violate the right to control our property and our bodies that we already enjoy; it does not require a legislature to contrive some new exception-riddled "right" that is really a claim on the behavior of others. The right to private property, and the subsequent privacy that that right yields, gives us a consistent, principled framework by which to judge privacy violations in all areas of life, not merely those related to the automated processing of information.

I cannot, for example, break into John's garage to see what kind of car he drives. Neither can I steal his mail (or e-mail) or credit card numbers, or plant video cameras in his bedroom. John's right to control his physical property thus affords him a considerable sphere of privacy, one that ends only where someone else's (including the government's) property begins. Thus, we have limited privacy when in a neighbor's home or walking down a public street—an obvious fact of life that belies claims of information ownership. After all, my watch is still mine when I wear it in my friend's apartment; if information were property, I would continue to own the information about myself that is disclosed there too. Most people would rightly assume that when I enter my friend's apartment I no longer have a reasonable expectation of privacy, that he will be free to tell other people about my visit, unless he promises not to. Visiting a store or a Web site is no different.

It is the role of the state to guard against violations of our right to hold property. If I break into John's garage, I should be arrested. Protecting citizens' lives and property is, in fact, the fundamental purpose of government. One way to think of it is that the government enjoys a monopoly on the use of force in society; citizens have delegated that power to the government so that their liberty and property may be secured. Yet because it has been granted the unique power to arrest and imprison people, the government must be strictly limited in the permissible uses of force. Indeed, in the privacy realm, the government poses a unique threat that private actors do not because an individual often has no recourse when an agent of the state violates her property, assuming that authorized procedures have been followed. Neither is she free to ignore government "requests" for information about herself, such as that requested on a census form or a tax return. Because of those powers to compel the disclosure of personal information, the behavior of the U.S. government is limited by law, most notably by the Fourth Amendment to the U.S. Constitution that protects citizens from unreasonable search and seizure.[50] Other more targeted laws, such as the Video Privacy Protection Act that limits the ability of law enforcement officials to demand access to personal video rental records, have been enacted for the same purpose.

Privacy in the "propertarian" framework is also protected through contracts, both explicit and implied. Take the example of a private online bookseller that compiles a computer database of its customers and sends that database to a direct marketing firm that is hired to send targeted mail solicitations to the people in the database. Although the direct marketer would like to sell the information in the bookseller's database to other retailers, the marketer signs a contract that prohibits it from sharing the database. The bookseller requires this contractual limitation on the use of its database because it does not want its competitors to be able take advantage of the knowledge it has about its customers. Privacy is thus protected by contract, not regulation.

Or consider the following real-world illustration. In June 2000 an online retail store named Toysmart filed for bankruptcy. In the process of liquidating assets to pay creditors, the company decided that it would sell valuable

Most people would rightly assume that when I enter my friend's apartment I no longer have a reasonable expectation of privacy, that he will be free to tell other people about my visit, unless he promises not to. Visiting a store or a Web site is no different.

All businesses are, in a sense, self-regulating. That does not mean that they are free to mislead or defraud consumers.

information about its customers and their purchasing habits, even though Toysmart had promised that such information would not be shared or sold. In other words, Toysmart had entered into the equivalent of a contract with its customers at the point of sale and was now threatening to break that contract. TRUSTe, the privacy-monitoring organization that had licensed Toysmart to display its seal, contacted the Federal Trade Commission about the impending breach of contract. The FTC warned Toysmart that selling the data would be a violation of the commitments it had made, and the company backed down.[51] The episode was quickly seized upon by advocates for new Internet privacy laws who argued that Toysmart was an example of why industry cannot be trusted to regulate itself on privacy. But in reality, the system had worked: it was contracts, not regulation per se, that protected privacy. And unlike Europe's legislatively granted privacy "rights," the idea of holding businesses accountable for their stated privacy policies, as a matter of contract enforcement, is firmly grounded in U.S. law. In *Cohen v. Cowles Media*, for example, the Supreme Court explicitly held that contracts not to disclose personal information are enforceable without conflicting with the First Amendment.[52]

Indeed, propertarian privacy protection has an impressive common law pedigree.[53] Before 1890 privacy in the United States was not legally separated from property. In *Boyd v. United States* (1886), for example, a businessman sued because agents had forcibly broken into his house, opened locked desks and boxes, and seized various papers. Justice Joseph Bradley wrote that the constitutional guarantees securing people in their persons, houses, papers, and effects "apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging in his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property."[54] More recently, in *Moore v. East Cleveland* (1977), the Court struck down a zoning law that prohibited a woman from living with two grandsons who were cousins.[55] Once again, the right to privacy—to live as one wishes within one's home without state interference—was intimately tied to property. Writing for the majority, Justice John Paul Stevens said that the test to be applied was "whether East Cleveland's housing ordinance is a permissible restriction on [Mrs. Moore's] right to use her property as she sees fit." Stevens concluded that it was not, writing that the city's "unprecedented ordinance constitutes a taking of property without due process and without just compensation." Mrs. Moore's privacy, in other words, was not a right standing apart from her right to own and control her property—the city could not invade Mrs. Moore's property, and thus her privacy was secure.

The propertarian approach is the legal framework that underpins what in the United States is called "self-regulation." But the term is misleading; all businesses are, in a sense, self-regulating. That does not mean that they are free to mislead or defraud consumers. On the contrary, businesses are bound by their contractual obligations, the threat of lawsuits, and the need to attract customers. If a business violates its privacy policy, it can be sued. If it does not have a privacy policy, it will go out of business if enough people care enough not to patronize it. A more accurate term is probably "market regulation," because it is primarily the economic choices of consumers that determine how companies may behave. Market regulation, based on firmly established property rights, offers as much or as little privacy as users desire, and it is not tied to any specific technology or process, such as "opt-in" or "opt-out." More important, however, is the fact that relying on property rights and contractual obligations as the primary vehicles for safeguarding privacy does not require the creation of a right to stop people from speaking about each other. Rather, we need only insist that people respect our space and honor their promises.

Free Speech vs. Data Protection

What implications does the directive's recognition of privacy as a "fundamental human

right," distinct from the right to own property and make contracts, have for freedom of speech? After all, there is necessarily a conflict between privacy and free expression whenever privacy is defined as the ownership of knowledge that others have about you. My "ownership" of information about myself requires that I have a right to stop you from using that information, which means that I can limit your speech. Such a right is especially problematic when the directive's restrictions on cross-border data flows are thrown into the mix.

Once again, the existence of personal Web sites illustrates the nature of the conflict. Strictly speaking, the directive does not seem to allow for the publication of any personally identifiable information on the Internet since such information would be viewable in countries that lack a government-enforced data protection regime equivalent to the one in Europe. Yet personal Web pages often contain personal information about, say, the author's friends and family members. It cannot simply be assumed that people named on such Web sites have granted permission for information about them to be posted. What if the personal Web page contains the author's opinions about some public figure, say the president of a major corporation? Could the CEO of an American company force a European citizen to take down an unauthorized biography that she had posted on the Web? The only way to enforce the directive in such cases would be to deny speech rights to the Web site's owner.

The compliance of European citizens' personal Web pages with the directive is, of course, a matter for local law enforcement and does not necessarily concern the U.S. government. But what about the personal Web page of a U.S. citizen who posts personally identifiable information about a European? Presumably, the poster would be in violation of the directive and could be sued for damages—though any judgment would obviously be difficult to enforce—even though the site owner's speech is protected under the First Amendment in the United States.

As UCLA law professor Eugene Volokh has noted: "The difficulty is that the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me. We already have a code of 'fair information practices,' and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is 'fair' or not."[56]

It is not sufficient to say that privacy laws like the directive are permissible because they can realistically regulate only "commercial" speech. First, the directive clearly applies to a good deal of speech that cannot be called commercial, such as personal Web sites and information collected by charities. Second, even if the exceptions contained in the directive are interpreted broadly enough to exempt the transfer of data by all entities except businesses, the restrictions remain unjustified. After all, every commercial transaction has at least two sides, a seller and a buyer. It is widely accepted that the buyer has the right to freely communicate the details of her experience with the seller, for example, to write a magazine review of a product or complain to *Consumer Reports*. Most Americans would consider it an egregious infringement of their right to free speech if a company or individual with which they had done business claimed ownership of the details of that experience.[57]

Similarly, we should not accept the claim—implicit in the directive and most proposed domestic privacy legislation—that the right to speak freely about a transaction is enjoyed only by the buyer. When a seller communicates the details of a transaction, that speech should be protected too. Not only does that conclusion appeal to widely held notions of fair play, but it is also true that society benefits greatly when businesses make public information about untrustworthy consumers. Reporting writers of bad checks or untrustworthy borrowers to credit bureaus, for example, lowers the cost of goods, services, and borrowing for honest consumers. Taken to its logical conclusion, protecting only the speech rights of buyers would make such valuable commercial communication impossible.

Market regulation, based on firmly established property rights, offers as much or as little privacy as users desire, and it is not tied to any specific technology or process, such as "opt-in" or "opt-out."

Businesses are not out to harm consumers; the reason they share information is to better home in on people who are interested in the goods and services that they provide.

It is important to remember that businesses are not out to harm consumers; the reason they share information is to better home in on people who are interested in the goods and services that they provide. In this way, the commercial use of personal information can significantly improve online experience by cutting down on the unsolicited junk mail that many people consider annoying. Moreover, businesses that target customers more effectively have lower marketing costs, which ultimately result in lower prices for consumers. Restricting commercial speech would eliminate those benefits without reducing any actual harm to consumers.

In any case, it is not permissible in the United States to regulate every form of commercial speech. In the vast majority of instances, courts have held that the right to freely communicate facts cannot, generally speaking, be denied, even to businesses. Where commercial speech has been restricted, the restriction has been limited to speech that actually proposes a commercial transaction, such as advertising. As Volokh has noted: "The Court's definition of 'commercial speech' . . . isn't (and can't be) simply speech that is sold as an article of commerce: Most newspapers, movies, and books are articles of commerce, too, but they remain fully protected."[58] Indeed, newspapers exist solely to sell details about the lives and careers of identifiable individuals, few of whom grant their permission for information about them to be published. Likewise, the sale or transfer of consumer information by an online retailer may be an act of commerce, but it is not the sort of "commercial speech" that may be regulated.

Given the enormous breadth of activities covered by the directive, and the uncountable number of daily violations, it is difficult to imagine European privacy authorities enforcing the law with substantial consistency. In other words, most infractions will simply be ignored, and most speech (commercial and other) will remain unaffected. Such necessarily inconsistent application of law, however, invites discretionary abuse by authorities. In Sweden, for example, critics of the Data Inspection Board—the regulatory body charged with enforcing Sweden's version of the EU data protection directive—report that it wields discretion in such a way as to "allow all activities which it likes, but disallow all activities which it dislikes."[59] Indeed, the law in Sweden specifically states that "minor" violations of the law will not be prosecuted.[60]

Nevertheless, restrictions on publishing personally identifiable information on the Internet have a chilling effect on speech. Since privacy bureaucrats possess nearly total prosecutorial discretion, it is not difficult to believe that they will ignore most violations while pursuing those that relate, for example, to the criticism of public officials online.

Are Consumers Demanding New Privacy Rights?

Much of the impetus for privacy-protecting legislation comes from consumer surveys that purport to show that a large majority of people are fearful of invasions of their privacy. If people do not trust that their privacy will be protected online, the reasoning goes, then electronic commerce will not be able to reach its "full potential." Yet there are good reasons to doubt the depth of public support for stringent privacy regulation. It is one thing to simply assert, when asked by a survey taker, that privacy is "important." It is much more instructive to observe how people actually behave when they are asked to place some monetary value on their personal data. Consumers often seem quite willing to divulge personal data in exchange for some benefit, such as free Internet access or the lower prices offered by grocery store loyalty programs. As cryptography expert Bruce Schneier writes in *Secrets and Lies*:

> People talk as if they don't want mega databases tracking their every spending move, but they are willing to get a frequent-flyer affinity card and give all that data away for one thousandth of a free fight to Hawaii. If McDonald's offered three free Big Macs for a DNA sample, there would be lines around the block.[61]

Research by Solveig Singleton of the Competitive Enterprise Institute and Jim Harper of Privicilla.org has shown that consumer surveys

on complex topics like privacy can be highly misleading.[62] Specifically, responses appear to be highly dependent on the precise wording of the survey. An oft-cited Business Week/Harris Interactive poll, "A Growing Threat," asked people how concerned they were that "the company you buy from uses personal information you provide to send you unwanted information." As Singleton and Harper point out, "No one wants to be sent *unwanted* information, so an overwhelming 78 percent of respondents said they were 'very' or 'somewhat' concerned about this."[63] By contrast, the Harris Interactive/Privacy Leadership Initiative asked more balanced questions and found that 54 percent of respondents would at least somewhat not appreciate e-mail *unrelated* to an initial purchase, while 63 percent would appreciate a related e-mail.[64]

Moreover, even if most Internet users are "concerned" about privacy, that does not necessarily mean that they are clamoring for new regulations. Indeed, most Internet users do not think much about the issue at all. Frank Newport, editor in chief of Gallup Polling, recently told Congress that only 16 percent of people report that they follow Internet privacy issues very closely, while "about half said that they weren't following the issue closely at all."[65]

Such findings appeal to common sense. It is difficult to be passionate about a "right" that is subject to numerous exceptions and qualifications and that we violate so freely in our daily lives. Unlike some other human rights, privacy is never absolute. Few people would deny that slavery and murder are *always* wrong. But privacy depends on the context—a breach of a privacy principle may be unacceptable in many circumstances but be considered perfectly reasonable in others. We may be annoyed when a person who knows something about us passes on that information without our permission, but few of us would hesitate to engage in that same behavior ourselves, and fewer still would feel guilty for having done so. And we all get our news from media whose very existence depends on being able to communicate information about other people—more often than not, without the permission of the data subject.

Of course, one of the major justifications for restrictions on uses of information is that electronic commerce will not reach its "full potential" unless the government acts to bolster consumer confidence. Yet indications are that, even though privacy and security rate as concerns for online shoppers, those concerns have not been a barrier to the robust growth of Internet commerce, as e-commerce revenues have continued to soar. The most recent report from the Commerce Department indicates that retail e-commerce sales in the first quarter of 2001 were $7.0 billion—up nearly 34 percent over the first quarter of 2000.[66] More than half of all Americans bought something online during the past holiday shopping season, up from only 20 percent in 1998. That upward trend is no surprise since businesses have a strong incentive to build consumer confidence by providing a trusted shopping experience that will keep customers happy. Why should government relieve businesses of that responsibility through regulation?[67]

Popular support for privacy regulation may be shallow, but it appears to be widespread. For many people, the idea that individuals have a property right in information about them seems intuitive. That, in part, explains the very high percentages of people who respond to surveys that ask whether they support legislation to protect their privacy. Yet this largely unexamined assumption leads to all sorts of harmful policy prescriptions and unintended costs, not least of which is a diminution of free speech rights.

Governmental Threats to Privacy

Unlike "real" property rights, the right to privacy under the directive does not generally extend to governmental uses of information. European governments remain free to collect, sell, disclose, store, and transfer any and all personal information without notice and are not required to allow citizens to access and correct information about themselves. Legislation has recently been proposed in Spain, for example, that would force Web sites to register with the government and require Web hosting companies to police site content.[68] The new Regulation of Investigatory Powers Act in Britain requires anyone communicating via the Internet to hand over the keys for decoding e-mails and other encrypted data.[69] In addition, Internet service

U.S. law provides citizens greater protection against government intrusions into their privacy than is generally the case in Europe.

providers (ISPs) are forced to install (at their own expense) hardware designed to monitor the traffic that crosses their systems and report suspicious messages to MI5, the British security service. Unlike authorities in the United States, authorities in Britain do not need to obtain a warrant signed by a judge. Finally, the European Commission is considering amending the directive itself to *require* increased collection of information. Under proposed amendments, ISPs throughout Europe, and perhaps beyond, would be forced to keep records of the Web sites that their customers visit, the time each person spends online, and certain details about e-mail exchanges. Industry groups have condemned the changes as "a retrograde step" that will compromise privacy and damage e-commerce.[70]

U.S. law provides citizens greater protection against government intrusions into their privacy than is generally the case in Europe. For Americans, who are generally more distrustful of government than are Europeans, the concentration on state misuses of personal information is largely a matter of common sense. As previously noted, the government holds a monopoly on the use of force in society—unique police and taxation powers that, when abused, can devastate an individual's life. A private business, by contrast, can only either attempt to convince an individual to enter into a transaction (as in advertising) or refuse to do business with an individual (as in the denial of credit). Although either of those private uses of personal information can be annoying or even harmful, they fall far short of the truly life-altering actions, such as imprisonment, that may be undertaken by governments. Moreover, private businesses are limited in the degree to which they can affect an individual by competition from other businesses. A wrongly denied bank loan, for example, represents a lost customer whom a competing lender would be happy to meet.

One of the most underreported aspects of the privacy debate, both in Europe and in the United States, is the inability of privacy advocates to point to any real harm caused by unregulated uses of personal information in the private sector, beyond the loss of privacy itself.

One of the most underreported aspects of the privacy debate, both in Europe and in the United States, is the inability of privacy advocates to point to any real harm caused by unregulated uses of personal information in the private sector, beyond the loss of privacy itself.

At the same time, many advocates inexplicably seem to minimize or ignore the ever-present threat of government abuse of personal information. In one recent example, a veteran of the U.S. Drug Enforcement Administration was charged with illegally selling sensitive information about private citizens that was pulled from federal and state law enforcement computers.[71] Such security breaches highlight the fact that the government rarely lives up to the standards that lawmakers say should apply to the private sector. The General Accounting Office audited computer security at the 25 largest federal agencies last year. Fully 18 agencies received a grade of C, and 7 were ranked as "failing." Agencies with the worst records included the Department of Justice, the Department of Labor, and the Department of Health and Human Services, all of which collect some of the most sensitive information about American citizens[72] Another GAO report on the privacy practices of federal government Web sites surveyed 65 Web sites and found that only 3 percent complied with all of the fair information principles that the FTC applies to commercial sites.[73]

Ironically, even the Commerce Department's Safe Harbor Web site has failed to secure confidential data. A recent story by *Wired News* uncovered the fact that visitors to the site could access confidential information—such as revenue, number of employees, and the European countries with which a firm does business—that companies provided to the government in order to qualify for Safe Harbor.[74] That information was available despite the fact that the Commerce Department's privacy statement says, "We will not share any personally identifying information you give us with any other government agency, private organization or the public, except with your consent or as required by law."[75]

How Is Safe Harbor Working So Far?

In a recent conversation with a member of the Federal Trade Commission, I was told that

the Safe Harbor agreement simply isn't an issue of great concern among Washington's privacy regulators these days. "It used to be that the first thing that everyone talked about when we got to work was Europe and Safe Harbor," this official said, "but today, that problem is completely off the radar screen."[76] The absence of press coverage of the Safe Harbor agreement seems to confirm that sentiment. Apart from an occasional story about how few companies are participating in the program, Safe Harbor has been virtually invisible in the media.

Safe Harbor's woes are not due only to neglect by U.S. officials and the mainstream media; both EU data authorities and American businesses have shown a similar lack of enthusiasm. Certainly, given the relative newness of Safe Harbor, it is too early to pass final judgment on the program. Evidence is mounting, however, that it may be in trouble.

Limited Enforcement

Table 1 was compiled from a Cato Institute survey of European data regulatory authorities. The question asked was, "Were any (and if so how many) companies fined or cited for transferring data from [the respective nation] out of Europe in the past?" Only four of the privacy offices contacted cited any confirmed violations of the directive, and those were quite minor in every case. Many other offices claimed to have no formal records of enforcement actions but said they "don't recall" any instances. Three privacy offices did not respond to the survey (or, in one case, did not seem to exist). The information presented here is far from comprehensive—especially considering the offices that refused to provide data or were unreachable—but the overall pattern is clear: the EU has not taken enforcement of the directive very seriously so far. Of the 16 privacy offices polled, only a handful reported any enforcement actions related to illegal data transfers at all.

Austria: The Austrian Data Protection Agency reported one case in which a company was charged with transferring data outside of Europe. The case involved a hospital that hired a firm in the United States to work on its patient files. The hospital was found to have violated Austrian law. However, the infraction was considered minor, and no actual misdeed was

If personal information is freely given on a regular basis, then perhaps EU netizens are less concerned about privacy than is generally assumed.

Table 1
Survey of Enforcement Actions Taken under the Directive

Country	Response to Survey (Yes = enforcement action taken)
EU Commission	Refused answer
Austria	Yes
Belguim	None known
Denmark	None known
Finland	Yes
France	No response
Germany	Yes
Greece	No response
Ireland	None known
Italy	None known
Luxembourg	Referred back to EU Commission
Netherlands	None known
Portugal	None known
Spain	No response
Sweden	None known
United Kingdom	Yes (prior to directive)

Of the 16 privacy offices polled, only a handful reported any enforcement actions related to illegal data transfers.

proved. The analogy given was that of driving without a license. The names of the companies involved are not mentioned in the response to the survey.

Finland: Finland's Data Protection Agency said that there were about 10 to 20 cases of companies being cited for transferring employee data outside of Europe. The official interviewed said that those cases usually involved data transferred to the United States, but no specific information on the countries involved was available.

Germany: The German Data Protection Agency reported two cases that occurred some years ago. The first involved the transfer of personal data to Detroit by Opel, the German subsidiary of General Motors. The second involved Volkswagen and its security arrangements for personal data. No information was available on what penalties, if any, were imposed.

United Kingdom: The UK data protection agency knew of one case in 1990—which predates the directive—of a company being charged with transferring data outside of Europe to a direct marketing operation in the United States. (The American company receiving the information was already under investigation by the U.S. Postal Service for fraud.) The UK company was served with a Transfer Prohibition Notice on the grounds that the transfer of personal data to the United States "would be likely to contravene or lead to a contravention of [Britain's] First, Second and Seventh Data Protection Principles."[77] The Office of the Information Commissioner knew of no other cases.

Survey Conclusion: It does not appear that companies in the European Union are very often cited or prosecuted for transferring data. It is true that in several countries companies are sometimes cited for violating the directive without ever facing criminal charges or fines. As long as the companies change their practices, the matter is dropped and is not a matter of public record. But on the basis of conversations with European officials, even such informal enforcement is rare, carried out on an ad hoc basis rather than in a systematic fashion. In other words, it seems very unlikely that a company currently operating in violation of the directive's provisions would face prosecution or an order to cut off data flows to third countries.

Observers on both continents have made similar assessments. Jeff Rohlmeier, a Commerce Department official who took part in the Safe Harbor negations, said that he had seen "no indication from the Europeans that they're planning on taking a hard line stance. They don't seem to be in a rush. They're willing to give Safe Harbor and the other side agreements an opportunity to prove successful."[78] Prof. Jacob Palme of the University of Stockholm even tried to provoke Swedish data protection authorities into enforcing Sweden's Personal Data Act of 1988, which is a precursor to the directive. He writes about his experiences on his personal Web site:

> In order to test the law, a number of people wrote Web pages containing various kinds of illegal texts, or asked the Data Inspection Board to consider the legality of such texts. For example, a Salvation Army soldier wrote a Web page with the title "Pinochet is a murderer" and then asked the public prosecutor to charge him with illegally publishing information about crimes (criminal personal information is regarded as specifically sensitive). I wrote to the Inspection Board and asked them if the public library, which on their Web page, has a biography by a plow-bill member, telling how he went to prison because of his illegal acts against weapons manufacturers.
>
> The Data Inspection Board in each case avoided following the law, by saying that they were, as asked by the Swedish government, making a study of how to resolve the conflict between the act and freedom of speech. This study was ready in 1999, and in the study, the Data Inspection Board proposes that "harmless" publishing on the Internet should be exempt from the law. Note that the term "freedom of speech" is never mentioned by the proposal.[79]

Thus, if there is any consistent application at all, enforcement of the directive appears to be triggered when uses of personal information rise above the vague standard of "harmlessness." No doubt most businesses and individuals think that their uses of personal data are harmless.

However, enforcement of the directive's provisions will not likely be delayed forever. The exact date by which non-EU organizations must comply is uncertain but extends, according to the EU Commission, at least through the conclusion of a one-year review period that ended on July 1, 2001. EU officials have reportedly told the U.S. government that this grace period will be extended. Whether the extension is due to benevolence or necessity, however, is not clear. What is clear is that the limited amount of resources devoted to privacy administration offices and the general lack of enforcement proceedings against European firms suggest that the EU has, at least so far, not taken the directive very seriously. Whether it will do so in the future remains an open question.

Limited Interest on the Part of U.S. Businesses

For their part, U.S. businesses have been giving Safe Harbor a wide berth. Table 2 lists the companies that have been Safe Harbor–certified as of the publication date of this paper.

It is obvious that a good number of the Safe Harbor–certified companies—such as TRUSTe and Privacy Leaders—are in the privacy business. Many others provide e-commerce or consulting services to other companies and are not directly involved in business-to-consumer commerce. There are almost no large businesses present. Of the listed companies, only Hewlett-Packard is a major player in the business-to-consumer world. (Microsoft has pledged to join but has yet to be certified.)

There are many reasons why U.S. businesses have been hesitant to join Safe Harbor. First, many of them may simply be unaware of its existence. Contrary to inside-the-beltway hubris, most businesses—especially smaller ones—have no need or inclination to follow the ins and outs of Washington policy debates. Second, the lack of enforcement by EU officials has limited the incentives for companies to take part. Some businesses consider it prudent to take a "wait and see" attitude, with little chance of facing sanctions, rather than commit themselves to potential liability and oversight by the FTC. Third, the Safe Harbor principles are more restrictive than generally accepted privacy practices in the United States. Compliance may require expensive upgrades to software and hardware, as well as rethinking routine business procedures. Finally, some firms believe that it may be easier for them to enter into privacy contracts with their European partners than to join Safe Harbor. The contract approach may be viewed as a way to avoid intrusive regulatory oversight in the United States.

Will Safe Harbor Fail?

Whatever the reasons, U.S. businesses have been and probably will continue to be skeptical of the benefits of joining Safe Harbor. In the meantime, trans-Atlantic e-commerce has continued to grow. Safe Harbor may have temporarily headed off a digital trade war between the United States and Europe, but it hardly seems to have resolved the underlying jurisdictional disputes over privacy and the regulation of personal information. The program has not been widely adopted by U.S. businesses and relies mostly on the continued willingness of European data protection authorities to ignore violations of their data laws. Such forbearance cannot be relied on indefinitely.

In addition, there continue to be internal European disputes over the legitimacy of the agreement. Last year the European Parliament rejected Safe Harbor, but the European Commission decided to implement it anyway.[80] Although the parliament's action was not legally binding, it does cast doubt on the long-term political viability of the deal. The European Commission is scheduled to complete a review of Safe Harbor before November 1, 2001. If the European Parliament demands a renegotiation of the deal, it could collapse. Many privacy officials are also unhappy with the arrangement because they think it lets American companies off the hook too easily. "Very frankly, we do not consider the safe harbor as a successful way to solve problems of data protection," says Giovanni Buttarelli, general secretary for the Italian Data Protection Commission, echoing the sentiments of many of his colleagues.[81]

Some businesses consider it prudent to take a "wait and see" attitude, with little chance of facing sanctions, rather than commit themselves to potential liability and oversight by the FTC.

Table 2
Safe Harbor Certification List

Adar International, Inc.	Numerical Algorithms Group, Inc.
Audits & Surveys Worldwide	Oak Technology
CapitalVenue	Pharmaceutical Product Development, Inc.
Cendant Data Services, Inc.	Privacy Leaders
Crew Tags Int'l	Qpass Inc.
Cybercitizens First Data Services, Inc.	Responsys
Decision Analyst, Inc.	Salesforce.com, Inc.
E-lection.com (LDE Inc.)	Software 2010 LLC
e2 Communications, Inc.	SonoSite, Inc.
enfoTrust networks	Strategic Marketing Corporation
Entertainment Software Rating Board Exult, Inc.	The Dun & Bradstreet Corporation
Genetic Technologies, Inc.	The USERTRUST Network LLC
Global-Z International, Inc.	TRUSTe
Global Medical Management, Inc.	United Information Group (c/o ASW)
HealthMedia, Inc.	USERFirst
Hewlett-Packard	USERTrust Inc.
Lebensart Technology Arizona, Inc.	USinternetworking, Inc.
Market Measures Interactive, LP	Virage, Inc.
Mediamark Research, Inc.	WellMed, Inc.
Naviant Marketing Solutions, Inc.	World Research, Inc.
NOP Automotive, Inc.	WorldChoiceTravel.com, Inc.

Source: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list, as of May 31, 2001.

Safe Harbor may have temporarily headed off a digital trade war between the United States and Europe, but it hardly seems to have resolved the underlying jurisdictional disputes over privacy and the regulation of personal information.

Skepticism about Safe Harbor has also been expressed on the U.S. side. The National Business Coalition on E-Commerce and Privacy, an industry lobbying group formed last year, complained to the Commerce Department about Safe Harbor shortly after the agreement was finalized. The group, which includes business powerhouses such as General Electric, Fidelity Investments, Home Depot, Seagrams, John Deere, and Aflac, said that national sovereignty has been compromised by the agreement, as the EU privacy principles exceed any domestic regulations imposed on U.S. businesses. "The safe harbor agreement in effect establishes a non-tariff trade barrier in that a U.S. person cannot do business with EU unless that person agrees to play by EU rules," a letter from the coalition states. "This trade barrier will disadvantage U.S. companies in relation to their competitors in other areas which do not have to abide by the principles of the EU directive."[82]

Compounding that skepticism is the fact that Safe Harbor does not cover U.S. financial institutions. On March 23 the Bush administration sent a letter to the European Commission objecting to a set of proposed privacy rules affecting financial service firms. In the letter, the Commerce and Treasury Departments said the proposed rules "impose unduly burdensome requirements that are incompatible with real-world operations."[83] David Aaron, the Clinton administration's chief negotiation on Safe Harbor, said that European officials went beyond what was agreed to in that deal. "Some of the things they added are obviously very troublesome," he said, backing the Bush administration's objections.[84] The administration's objectives come at a time when U.S. financial services firms are increasingly pressing European officials to determine that U.S. data privacy measures in that sector are adequate to protect EU citizens—a move that seems unlikely.[85]

Given internal dissatisfaction with Safe Harbor in Europe, its failure to include the financial service sector, and the general lack of response on the part of U.S. businesses, the future of Safe Harbor is shaky indeed. It is perhaps too soon to conclude that Safe Harbor is doomed, but given the many strikes against the agreement, prudence suggests that the U.S. government should give some thought to what to do if, or when, it collapses.

Market Privacy or International Regulations?

The most encouraging news on the privacy front comes from the private sector, which is racing to develop tools that consumers can use to protect information about themselves. Although those innovations are not dependent on international negotiations or treaties, they do have the potential to help ameliorate the tensions between governments. New market-based solutions to protecting privacy are crucial because many of the differences between the United States and European Union are insurmountable. The difficulties with applying the directive against small Web sites based wholly in foreign countries are, for example, probably so great as to make enforcement impossible. Small Web sites will simply flout European law, and there is little that data authorities can do about it.

Fortunately, the danger to European consumers is far less than is often imagined. For one thing, it seems safe to assume that privacy-skittish Europeans will be unlikely to divulge their personal data to Web sites that do not fall under European jurisdiction. If, contrary to this expectation, personal information is freely given on a regular basis, then perhaps EU netizens are less concerned about privacy than is generally assumed. Beyond such consumer self-restraint, there is the range of "good privacy practice" certification services that have sprung up to meet the demand by online businesses to reassure customers that information about them will not be used for unapproved purposes. Several of those programs, such as TRUSTe and the Better Business Bureau Online, are already in use by the most heavily trafficked sites on the Web.

However, seal programs are no longer the only places that privacy-conscious consumers can turn. Such programs are increasingly being supplemented by a range of new services and technologies that allow online shoppers to conduct anonymous transactions. Securicor, Zeroknowledge.com, SafeWeb.com, and Anonymizer.com are among the companies that provide various degrees of privacy for Internet users, either free or for a fee.

British-based Securicor, for example, allows EU shoppers to protect their privacy with greater certainty than relying on legal safeguards. Users register their personal information with Securicor, including name, address, e-mail address, and credit card numbers. They are then able to shop either at a Securicor virtual mall or at outside retailers' Web sites. When a user decides to make a purchase, he is taken to the Securicor Web site, which authenticates the buyer and processes the transaction. The end retailer never knows who places the order or any personal details about the customer. The only information received by the retailer is the type and quantity of items bought; payment is made by Securicor. For additional privacy, customers can have their goods delivered by Securicor Omega Express, the company's private delivery service.[86] In the United States a company called iPrivacy is offering services similar to those offered by Securicor.

Another privacy-enhancing technology on the horizon is P3P, the Platform for Privacy Preferences, a project of the World Wide Web Consortium.[87] P3P is a set of standardized protocols that a merchant can embed in his Web site. The P3P protocols describe, in a machine-readable format, precisely what uses will be made of personal information collected at the site: whether the information will be stored, sold, traded, or used for marketing purposes. On the consumer end, P3P-enabled Web browsers read the privacy information embedded in the site and compare it with a series of multiple choice questions answered by the user. If the P3P protocols indicate that the site has a personal data policy that matches or exceeds the

It is perhaps too soon to conclude that Safe Harbor is doomed, but given the many strikes against the agreement, prudence suggests that the U.S. government should give some thought to what to do if, or when, it collapses.

user's stated preferences, then nothing happens. If, however, the site's privacy policy indicates that information will be used in an unapproved manner—or if the site does not use P3P—then the user will receive an appropriate warning.

Although the details of P3P are still being worked out, the dominant players in the browser market, Microsoft and Netscape, have already committed to incorporate the finalized system into their products. When that happens—which it reportedly will near the end of 2001—P3P will make it significantly easier for online shoppers to dictate how information about them will be used.

P3P is not without limitations. It will not, for instance, protect a Web user in Europe from all transfers of her data to third parties, nor will it ensure that she has a right to access and correct disputed information. In short, P3P deals only with privacy practice *disclosure*; it does not confer any special rights on the data subject beyond the inherent right not to visit a site with an unfavorable privacy policy. That is no small feat: by automating the disclosure process, P3P can ensure that a person never inadvertently gives out personal information to the wrong Web site. P3P promises to take the confusion out of currently obscure, legalistic privacy policies and provide a warning about sites that lack any privacy policy at all. Under a perfectly functioning P3P system, it seems reasonable to assume that all disclosures of personal information are made with at least the implicit consent of the data subject.

With the proliferation of privacy-protecting technologies—including Securicor, iPrivacy, and P3P—data regulations such as the directive are already beginning to look dated.

Would P3P obviate the need for agreements, such as Safe Harbor, that seek to bridge the gap between the different approaches to information management in various parts of the world? As with so many questions about the directive, the answer is unclear. If a Web site is coded for P3P, can a company assume that whatever information a European decides to volunteer has been given with the "unambiguous consent" required by Article 26? If so, that information could be freely transferred out of Europe. What of people with older software that is not P3P enabled? Should owners of U.S. Web sites refuse to do business with them?

There are no clear answers to such questions. One thing, however, seems certain: with the proliferation of privacy-protecting technologies—including Securicor, iPrivacy, and P3P—data regulations such as the directive are already beginning to look dated. Consumers are becoming ever more empowered to make their own choices about privacy. It is hard to see why, in such a world, the directive is needed to protect consumers. As time goes by, depending on how the directive is ultimately implemented, the protectionist aspects of European privacy law may be increasingly difficult to justify.

Conclusion

The EU Data Protection Directive is a confusing document that is based on an inherently flawed set of assumptions. It is only by carving out a large number of exceptions to its core principles, and by not strictly enforcing them, that the directive has not yet imploded. But despite its many shortcomings, the directive is likely to remain the law of the land within Europe for the foreseeable future. Policymakers in the United States will have to deal with the directive whether they like it or not.

It was understandable that the United States negotiated Safe Harbor as a first attempt to bridge the differences between the U.S. and the European approaches to regulating the flow of personal information, particularly given the economic damage that the directive could cause. But so far, judging by the paltry number of companies that have been certified and the continuing dissatisfaction of some European officials, Safe Harbor does not seem to be working. It is simply not worth the effort for most U.S. companies to sign up. At best, most large multinational companies will wait to see if their operations are ever seriously threatened, and small businesses will never sign up because there is no practical way for Europe to enforce restrictions against them.

It would therefore be prudent for U.S. policymakers to begin contemplating what they will do in a post–Safe Harbor world. The first thing that U.S. policymakers must realize is that Europe does indeed have the right to set its own privacy policies, even when such polices are

costly and unnecessary. At the same time, however, Europe is bound by international trade commitments that require it to apply permissible trade restrictions in a manner that does not discriminate against countries or businesses. Because the directive potentially falls short in this area, the United States should not hesitate to hold European countries to their pledges to maintain open markets. If the directive is enforced in such a way as to put U.S. companies at an unfair disadvantage—which is entirely possible—the United States should not hesitate to defend its interests through the multilateral dispute resolution mechanism of the WTO.

At the same time, it is important for policymakers to recognize that a lack of regulation is not the same thing as a lack of privacy protection. In a market economy, businesses produce the goods and services that consumers demand, not because they are forced to do so by the government, but because they will fail if consumers are not happy. Privacy is no different in that regard: if consumers desire it, businesses will provide it. People have different appetites for privacy and should be free to transact with businesses that share information and with those that do not. Real harms, such as fraud or theft, should be punished, but primarily through torts and existing criminal law. If new rules or enforcement programs prove necessary in some cases, those programs should be as narrowly targeted as possible.

It is to be hoped that the policing role of government will be minimal. Indeed, new technologies and private privacy certification systems are already rendering moot many debates over privacy policy. Seal programs already exist that give privacy-conscious consumers an easy way to determine if the Web sites they visit offer the level of privacy they prefer. Soon P3P will make avoiding sites that share information even easier. (Incidentally, it is no accident that such market innovations are being developed mostly in the United States rather than in Europe.)

Relying on technology and market incentives, rather than regulation, to protect privacy empowers individual consumers to make their own choices. By contrast, the one-size-fits-all regulatory model of privacy protection forces everyone—even people who are willing to share personal information—to bear the costs of compliance. The less information businesses have about their customers and potential customers, the higher the cost of goods and services will be. It is simply not fair to insist that everyone share that burden of inefficiency.

Finally, it is important to remember that the philosophy of the directive is inimical to free speech traditions in the United States. The exchange of factually accurate information about people and events is protected speech under the First Amendment. If we accept the principle that people have a broad-based right to restrict what others say about them, even when the things being said are true and no laws were violated in the course of obtaining the information, then we will have gone a long way toward weakening one of the key pillars of our free society.

In short, U.S. policymakers should recognize the many advantages that flow from a market-based privacy regime and, further, that the United States has a sovereign right to determine its own polices in this area. They must not allow themselves to be bullied into adopting EU-style privacy regulations designed to avoid sanctions under the directive. Safe Harbor should not be abandoned today, but neither should it be counted on as a secure port in future privacy storms.

Notes

1. See European Union, "Data Protection Directive," http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html. Cited hereafter as Directive.

2. The United States has a wide range of sectoral privacy regulations, including the Electronic Communications Privacy Act, the Video Privacy Protection Act, the Right to Financial Privacy Act, the Driver's Privacy Protection Act, the Privacy Protection Act of 1980, the Family Education Rights and Privacy Act, substance abuse privacy laws, and the Veterans Administration Health Privacy Act.

3. U.S. Department of Health, Education and Welfare, "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," 1973, http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

If the directive is enforced in such a way as to put U.S. companies at an unfair disadvantage—which is entirely possible—the United States should not hesitate to defend its interests through the multilateral dispute resolution mechanism of the WTO.

4. 5 U.S.C. § 552a, http://www.usdoj.gov/04foia/privstat.htm.

5. For the full text of the guidelines, see Organization for Economic Cooperation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," September 23, 1980, http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

6. http://www.datenschutz-berlin.de/gesetze/internat/aen.htm.

7. Council of Europe, "Convention on the Protection of Individuals with Regard to the Automatic Processing of Personal Data Convention," ETS no. 108, Strasbourg, 1981, http://conventions.coe.int/treaty/en/Treaties/Html/108.htm.

8. Ibid. Emphasis added.

9. David Smith, Testimony before the House Energy and Commerce Committee, 107th Cong., 1st sess., March 8, 2001, http://www.house.gov/commerce/hearings/03082001-49/ Smith101 .htm.

10. Directive, Article 1(2), reads in full: "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1." The bracketed text is taken from Directive, Article 1(1).

11. Ibid., Article 3(1).

12. Ibid., Article 3(2).

13. See http://www.e-mps.org.

14. Financial Services Coordinating Council, "Study Finds European Union Privacy Directive Would Cost U.S. Consumers Time, Money," Press release, April 30, 2001, http://biz.yahoo.com/prnews/010430/dcm026.html.

15. Robert W. Hahn, "An Assessment of the Costs of Proposed Online Privacy Legislation," American Enterprise Institute–Brookings Institution Joint Center for Regulatory Studies Paper, May 7, 2001, http://www.actonline.org/pubs/HahnStudy.pdf.

16. For a fuller exploration of this danger, see Shane Ham and Robert D. Atkinson, "Online Privacy and a Free Internet: Striking a Balance," Progressive Policy Institute Policy Report, April 2001, http://www.ndol.org/documents/E-Privacy2.pdf.

17. See, for example, Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (Washington: Brookings Institution, 1998).

18. Quoted in William New, "Tauzin: European Data Protection May Violate WTO," *National Journal's Technology Daily*, March 8, 2001.

19. See quotes from by Rep. Edward Markey (D-Mass.) in ibid.

20. See, for example, Jonathan Winer, Testimony before the House Subcommittee on Commerce, Trade, and Consumer Protection, 107th Cong., 1st sess., March 8, 2001, in which he calls the directive "the EU's version of the Helms-Burton Act."

21. Kate Scribbins, "Privacy@net: An International Comparative Study of Consumer Privacy on the Internet," Consumers International report, January 2001, http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf.

22. See, for example, http://www.flintcarrepair.co.uk;https://www.dnet.co.uk/nigelhoskin; http://www.halloweenilluminations.com; and http://www.intercept.co.uk.

23. World Trade Organization, "United States—Import Prohibition of Certain Shrimp and Shrimp Products," WTO Panel Report, May 15, 1998, 7.45.

24. Ibid., 7.49.

25. Ibid., 7.62.

26. World Trade Organization, Appellate Body Report WT/DS58/AB/R, October 12, 1998, p. 63, 161. Emphasis in original.

27. See http://www.wto.org/english/thewto_e/whatis_e/tif_e/bey5_e.htm.

28. Quoted in "EU Privacy Law Seen as Threat to US Businesses," Agence France Presse, November 30, 1998.

29. European Union, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, "Opinion 2/99 on the Adequacy of the International Safe Harbour Principles," issued by the U.S. Department of Commerce on April 19, 1999.

30. Mike Smith, "EU and US Agree on Data Protection," *Financial Times*, March 15, 2000.

31. Quoted in "Europe OKs U.S. Privacy Pact," *Wired News*, July 27, 2000, http://www.wired.com/news/politics/0,1283,37839,00.html.

32. Quoted in Juliana Gruenwald, "Stormy Seas Ahead over 'Safe Harbor,'" *Interactive Week*, October 30, 2000, http://www.zdnet.com/zdnn/stories/news/0,4586,2646060,00.html.

33. "Welcome to the Safe Harbor," http://www.export.gov/safeharbor.

34. Safe Harbor Overview, http://www.export.gov/safeharbor.

35. Ibid.

36. Ibid.

37. Ibid.

38. U.S. Department of Commerce, "Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law," Dispatch to the European Commission, July 14, 2000, http://www.ita.doc.gov/td/ecom/PRIVACYDAMAGESFINAL.htm.

39. See Federal Trade Commission Act, 15 U.S.C. § 5.

40. Quoted in "Trough Thick and Thin; E-Commerce Issues in the New 'New Economy,'" *Texas Lawyer*, April 16, 2001, p. 25.

41. See http://www.truste.org; and http://www.bbbonline.org.

42. Quoted in Gruenwald.

43. Quoted in ibid.

44. See http://www.toadsuck-usa.com/a-chkform1.html.

45. Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress," May 2000, http://www.ftc.gov/os/2000/05/index.htm#22.

46. Directive, Article 26(c).

47. Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), quoted in Toby Lester, "The Reinvention of Privacy," *Atlantic Monthly*, March 2001, electronic version.

48. David Banisar, "Privacy and Data Protection around the World," Paper presented at the 21st Annual Conference on Privacy and Personal Data Protection, sponsored by Office of the Hong Kong Privacy Commissioner for Personal Data, Hong Kong, September 13, 1999, http://www.pco.org.hk/download_doc/banisar-paper.doc.

49. Directive, Article 1(1).

50. The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

51. See http://www.ftc.gov/opa/2000/07/toysmart2.htm.

52. *Cohen v. Cowles Media*, 501 U.S. 663 (1991).

53. See Sheldon Richman, "Dissolving the Inkblot: Privacy as Property Right," *Cato Policy Report* 15, no. 1 (January–February 1993): 1.

54. *Boyd v. United States*, 116 U.S. 616 (1886).

55. *Moore v. East Cleveland*, 431 U.S. 494 (1977).

56. Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You," http://www.law.ucla.edu/faculty/volokh/privacy.html.

57. For more on this idea, see Solveig Singleton, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," Cato Institute Policy Analysis no. 295, January 22, 1998.

58. Volokh, § IV(A).

59. Jacob Palme, "European Data Directive Censors Anti-Bank, Animal Rights Activists," politechbot.com, May 15, 2000, http://www.politechbot.com/p-01165.html.

60. For the full text of Sweden's Personal Data Act (in English), see http://www.datainspektionen.se/PDF-filer/ovrigt/pul-eng.pdf.

61. Bruce Schneier, *Secrets and Lies* (New York: John Wiley & Sons, 2000), p. 65.

62. Solveig Singleton and Jim Harper, "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," Competitive Enterprise Institute Monograph, June 1, 2001, http://www.cei.org/MonoReader.asp?ID=1526.

63. Ibid., p. 2.

64. Reported in ibid.

65. Frank Newport, Testimony before the House Committee on Energy and Commerce, 107th Cong., 1st sess., May 8, 2001, http://energy-commerce.house.gov/107/hearings/05082001Hearing209/Newport307.htm.

66. http://www.census.gov/mrts/www/current.html.

67. For more on the idea of privacy regulation as corporate welfare, see http://www.privicilla.org/corpratewelfare.htm.

68. Julia Scheeres, "Fears of a Website Inquisition," *Wired News*, May 29, 2001,

http://www.wired.com/news/print/0,1294,44110,00.html.

69. See http://www.hmso.gov.uk/acts/acts2000/20000023.htm.

70. Lea Patterson, "CBI Attacks EU Net 'Log' Plans," *Times* (London), June 25, 2001, http://www.thetimes.co.uk/article/0,,5-2001213193,00.html.

71. Kevin Poulsen, "DEA Agent Charged with Selling Data," *SecurityFocus*, January 22, 2001, http://www.securityfocus.com/news/142.

72. U.S. General Accounting Office, "Computer Security: Critical Federal Operations and Assets Remain at Risk," T-AIMD-00-314, September 11, 2000, http://www.gao.gov/new.items/ai00314t.pdf.

73. U.S. General Accounting Office, "Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles," AIMD-00-296R, September 11, 2000, http://www.gao.gov/new.items/ai00296r.pdf.

74. Declan McCullagh, "'Secure' U.S. Site Wasn't Very," *Wired News*, July 6, 2001, http://www.wired.com/news/print/0,1294,45031,00.html.

75. http://osecnt13.osec.doc.gov/public.nsf/docs/privacy-statement.

76. Conversation with FTC commissioner Orsen Swindle at the Cato Institute, January 29, 2001.

77. David Smith, assistant information commissioner, UK, fax of February 21, 2001.

78. Quoted in Peronet Despeignes, "US and EU Clash on Privacy," *Financial Times*, March 27, 2001.

79. Jacob Palme, "Freedom of Speech, The EU Data Protection Directive and the Swedish Personal Data Act," personal Web page, June 9, 2000, http://www.dsv.su.se/jpalme/society/eu-data-directive-freedom.html.

80. See Anandashankar Mazumdar, "Experts See Indifference to Safe Harbor as Indication U.S. Firms Take Privacy Lightly," *International Trade Reporter* 18, no. 16 (April 19, 2001): 618–19.

81. Quoted in Gruenwald.

82. Quoted in Chet Dembeck, "EU Privacy Pact Held Hostage by Powerful Few," *E-Commerce Times*, April 7, 2000, http://www.ecommercetimes.com/perl/story /?id=2920.

83. Quoted in Glenn R. Simpson, "U.S. Objects to EU's Proposed Rules Affecting Trans-Atlantic E-Commerce," *Wall Street Journal*, March 27, 2001.

84. Quoted in ibid.

85. See "U.S. Industry Engages EU on Data Privacy, after EU Rejects Delay," *Inside U.S. Trade*, May 18, 2001.

86. Carlos Grande, "The Value of Customer Data," *Financial Times*, November 28, 2000. See also http://www.securicor.com.

87. For more information on the P3P project, see http://www.w3.org/P3P.

Trade Briefing Papers from the Cato Institute

"Missing the Target: The Failure of the Helms-Burton Act" by Mark A. Groombridge (no. 12, June 5, 2001)

"The Case for Open Capital Markets" by Robert Krol (no. 11, March 15, 2001)

"WTO Report Card III: Globalization and Developing Countries" by Aaron Lukas (no. 10, June 20, 2000)

"WTO Report Card II: An Exercise or Surrender of U.S. Sovereignty?" by William H. Lash III and Daniel T. Griswold (no. 9, May 4, 2000)

"WTO Report Card: America's Economic Stake in Open Trade" by Daniel T. Griswold (no. 8, April 3, 2000)

"The H-1B Straitjacket: Why Congress Should Repeal the Cap on Foreign-Born Highly Skilled Workers" by Suzette Brooks Masters and Ted Ruthizer (no. 7, March 3, 2000)

"Trade, Jobs, and Manufacturing: Why (Almost All) U.S. Workers Should Welcome Imports" by Daniel T. Griswold (no. 6, September 30, 1999)

"Trade and the Transformation of China: The Case for Normal Trade Relations" by Daniel T. Griswold, Ned Graham, Robert Kapp, and Nicholas Lardy (no. 5, July 19, 1999)

"The Steel 'Crisis' and the Costs of Protectionism" by Brink Lindsey, Daniel T. Griswold, and Aaron Lukas (no. 4, April 16, 1999)

"State and Local Sanctions Fail Constitutional Test" by David R. Schmahmann and James S. Finch (no. 3, August 6, 1998)

"Free Trade and Human Rights: The Moral Case for Engagement" by Robert A. Sirico (no. 2, July 17, 1998)

"The Blessings of Free Trade" by James K. Glassman (no. 1, May 1, 1998)

From the Cato Institute Briefing Papers Series

"The Myth of Superiority of American Encryption Products" by Henry B. Wolfe (no. 42, November 12, 1998)

"The Fast Track to Freer Trade" by Daniel T. Griswold (no. 34, October 30, 1997)

"Anti-Dumping Laws Trash Supercomputer Competition" by Christopher M. Dumler (no. 32, October 14, 1997)

Trade Policy Analysis Papers from the Cato Institute

"Trade, Labor, and the Environment: How Blue and Green Sanctions Threaten Higher Standards" by Daniel T. Griswold (no. 15, August 2, 2001)

"Coming Home to Roost: Proliferating Antidumping Laws and the Growing Threat to U.S. Exports" by Brink Lindsey and Dan Ikenson (no. 14, July 30, 2001)

"Free Trade, Free Markets: Rating the 106th Congress" by Daniel T. Griswold (no. 13, March 26, 2001)

"America's Record Trade Deficit: A Symbol of Economic Strength" by Daniel T. Griswold (no. 12, February 9, 2001)

"Nailing the Homeowner: The Economic Impact of Trade Protection of the Softwood Lumber Insudstry" by Brink Linsey, Mark A. Groombridge, and Prakash Loungani (no. 11, July 6, 2000)

"China's Long March to a Market Economy: The Case for Permanent Normal Trade Relations with the People's Republic of China" by Mark A. Groombridge (no. 10, April 24, 2000)

"Tax Bytes: A Primer on the Taxation of Electronic Commerce" by Aaron Lukas (no. 9, December 17, 1999)

"Seattle and Beyond: A WTO Agenda for the New Millennium" by Brink Lindsey, Daniel T. Griswold, Mark A. Groombridge and Aaron Lukas (no. 8, November 4, 1999)

"The U.S. Antidumping Law: Rhetoric versus Reality" by Brink Lindsey (no. 7, August 16, 1999)

"Free Trade, Free Markets: Rating the 105th Congress" by Daniel T. Griswold (no. 6, February 3, 1999)

"Opening U.S. Skies to Global Airline Competition" by Kenneth J. Button (no. 5, November 24, 1998)

"A New Track for U.S. Trade Policy" by Brink Lindsey (no. 4, September 11, 1998)

"Revisiting the 'Revisionists': The Rise and Fall of the Japanese Economic Model" by Brink Lindsey and Aaron Lukas (no. 3, July 31, 1998)

"America's Maligned and Misunderstood Trade Deficit" by Daniel T. Griswold (no. 2, April 20, 1998)

"U.S. Sanctions against Burma: A Failure on All Fronts" by Leon T. Hadar (no. 1, March 26, 1998)

From the Cato Institute Foreign Policy Briefing Papers Series

"Washington's Iron Curtain against East European Exports" by James Bovard (no. 15, January 7, 1992)

"Dump Our Anti-dumping Law" by Michael S. Knoll (no. 11, July 25, 1991)

"A Mexican View of North American Free Trade" by Roberto Salinas-Leon (no. 9, May 21, 1991)

"Banking on Poverty: An Insider's Look at the World Bank" by Michael H. K. Irwin (no. 3, September 20, 1990)

From the Cato Institute Policy Analysis Series

"New Asylum Laws: Undermining an American Ideal" by Michele R. Pistone (no. 299, March 24, 1998)

"Market Opening or Corporate Welfare? 'Results-Oriented' Trade Policy toward Japan" by Scott Latham (no. 252, April 15, 1996)

"The Myth of Fair Trade" by James Bovard (no. 164, November 1, 1991)

"Why Trade Retailiation Closes Markets and Impoverishes People" by Jim Powell (no. 143, November 30, 1990)

"The Perils of Managed Trade" by Susan W. Liebeler and Michael S. Knoll (no. 138, August 29, 1990)

"Economic Sanctions: Foreign Policy Levers or Signals?" by Joseph G. Gavin III (no. 124, November 7, 1989)

"The Reagan Record on Trade: Rhetoric vs. Reality" by Sheldon Richman (no. 107, May 30, 1988)

"Our Trade Laws Are a National Disgrace" by James Bovard (no. 91, September 18, 1987)

"What's Wrong with Trade Sanctions" by Bruce Bartlett (no. 64, December 23, 1985)

Other Trade Publications from the Cato Institute

James Gwartney and Robert Lawson, *Economic Freedom of the World: 2001 Annual Report* (Washington: Cato Institute, 2001)

China's Future: Constructive Partner or Emerging Threat? ed. Ted Galen Carpenter and James A. Dorn (Washington: Cato Institute, 2000)

Peter Bauer, *From Subsistence to Exchange and Other Essays* (Washington: Cato Institute, 2000)

James Gwartney and Robert Lawson, *Economic Freedom of the World: 2000 Annual Report* (Washington: Cato Institute, 2000)

Global Fortune: The Stumble and Rise of World Capitalism, ed. Ian Vásquez (Washington: Cato Institute, 2000)

Economic Casualties: How U.S. Foreign Policy Undermines Trade, Growth, and Liberty, ed. Solveig Singleton and Daniel T. Griswold (Washington: Cato Institute, 1999)

China in the New Millennium: Market Reforms and Social Development, ed. James A. Dorn (Washington: Cato Institute, 1998)

The Revolution in Development Economics, ed. James A. Dorn, Steve H. Hanke, and Alan A. Walters (Washington: Cato Institute, 1998)

Freedom to Trade: Refuting the New Protectionism, ed. Edward L. Hudgins (Washington: Cato Institute, 1997)

CENTER FOR TRADE POLICY STUDIES

The mission of the Cato Institute's Center for Trade Policy Studies is to increase public understanding of the benefits of free trade and the costs of protectionism. The center publishes briefing papers, policy analyses, and books and hosts frequent policy forums and conferences on the full range of trade policy issues.

Scholars at the Cato trade policy center recognize that open markets mean wider choices and lower prices for businesses and consumers, as well as more vigorous competition that encourages greater productivity and innovation. Those benefits are available to any country that adopts free-trade policies; they are not contingent upon "fair trade" or a "level playing field" in other countries. Moreover, the case for free trade goes beyond economic efficiency. The freedom to trade is a basic human liberty, and its exercise across political borders unites people in peaceful cooperation and mutual prosperity.

The center is part of the Cato Institute, an independent policy research organization in Washington, D.C. The Cato Institute pursues a broad-based research program rooted in the traditional American principles of individual liberty and limited government.

For more information on the Center for Trade Policy Studies, visit www.freetrade.org.

Other Trade Studies from the Cato Institute

"Trade, Labor, and the Environment: How Blue and Green Sanctions Threaten Higher Standards" by Daniel T. Griswold, Trade Policy Analysis no. 15 (August 2, 2001)

"Coming Home to Roost: Proliferating Antidumping Laws and the Growing Threat to U.S. Exports" by Brink Lindsey and Dan Ikenson, Trade Policy Analysis no. 14 (July 30, 2001)

"Missing the Target: The Failure of the Helms-Burton Act" by Mark A. Groombridge, Trade Briefing Paper no. 12 (June 5, 2001)

"Free Trade, Free Markets: Rating the 106th Congress" by Daniel T. Griswold, Trade Policy Analysis no. 13 (March 26, 2001)

"The Case for Open Capital Markets" by Robert Krol, Trade Briefing Paper no. 11 (March 15, 2001)

"America's Record Trade Deficit: A Symbol of Economic Strength" by Daniel T. Griswold, Trade Policy Analysis no. 12 (February 9, 2001)

"Nailing the Homeowner: The Economic Impact of Trade Protection of the Softwood Lumber Industry" by Brink Lindsey, Mark A. Groombridge, and Prakash Loungani, Trade Policy Analysis no. 11 (July 6, 2000)