ECONOMIC FREEDOM PROJECT

PRIVACY AS A TRADE ISSUE: GUIDELINES FOR U.S. TRADE NEGOTIATORS

By Solveig Singleton

EFP02-02 March 18, 2002

The Heritage Foundation

NOTE: Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Privacy as a Trade Issue: Guidelines for U.S. Trade Negotiators

Solveig Singleton

Privacy, known in Europe as "data protection," looms as a serious trade issue between the United States and Europe. If the establishment of the World Trade Organization (WTO) represents an international statement in favor of global free trade, the European nations' data protection laws represent a threat to that regime. Currently at issue are countries' regulations governing financial privacy. Consumers and businesses on both sides of the Atlantic will benefit if the United States maintains a strong stand in trade negotiations to protect the free flow of information across borders and within the United States.

Under a European Union (EU) regime known as the Data Protection Directive, which took effect in 1998, an EU member nation may refuse to allow a U.S. firm operating in Europe to transfer personal data out of the country if privacy protection for the firm's data in the United States is determined to be inadequate. In July 2000, the U.S. Department of Commerce and European officials negotiated a "safe harbor" agreement describing what steps U.S. firms must take to satisfy the standard of "adequacy."[1] The safe harbor agreement took effect in November 2000, but it did not apply to financial services companies. Financial services companies, Bush Administration Treasury representatives, and European officials carried out negotiations throughout 2001, with the Bush Administration rejecting Europe's first proposals.[2]

These negotiations are the latest stage in the evolution of privacy as a trade issue. U.S. lawmakers face pressure to reject the American tradition of the free flow of information and to develop a top-down regulatory regime for the governance of privacy and data. Some of this pressure stems from the differences between the EU countries and the United States: The EU countries have enacted broad data protection rules; the United States has not. Canada also has enacted a data protection regime similar to that in Europe.

The differential presents a classic trade problem. Country X prohibits or heavily regulates certain activity; country Y does not. The activity continues and expands in country Y, while representatives in country X become more frustrated. What should these countries do? Tolerate the regulatory arbitrage? Sanction country X to remove its regulations, or sanction country Y to adopt them? In large part, the answer depends on whether policymakers think that coun-

1. Details of the negotiations leading up to the safe harbor accord are described in Aaron Lukas, "Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive," Cato Institute *Trade Policy Study* No. 16, 2001, p. 11–13.
2. Thomas A. Hemphill, "Information Technology and Innovation Policy in the Bush Era," *Business Horizons*, January 1, 2002.

try Y or country X is doing the right thing. The assumption often is made that by passing data protection laws, the European nations are doing the right thing and the United States is not.

On close examination, this assumption is flawed. U.S. rules have favored the free flow of truthful information about real people and real events throughout the economy, with privacy as a carefully crafted exception rather than a default rule, and with protections for sensitive information that affects national security and defense. Only by protecting the free flow of information can consumers and firms around the world reap the full benefits of free trade.

PRIVACY AS A TRADE ISSUE

It may seem counterintuitive to consider privacy a trade issue. One might think that in regulating U.S. firms' compliance with data protection rules within European nations, those firms are merely being asked to comply with local law, and that familiar requirement does not usually raise trade issues. But this analysis is simplistic. The fact is that data protection rules do affect international trade.

A Historical Overview. Since the horrors of the Holocaust, when census data were used to identify the households of ethnic and religious targets, Europeans have had a heightened sensitivity to privacy. As the national welfare states grew throughout Europe in the 1970s, the first "data protection" rules were enacted. The German province of Hesse passed the first law in 1970 in reaction to the computerization of information. Sweden passed the first national data protection law in 1973 at the time the country adopted national identity cards.

As these national laws were adopted, trade issues began to arise. For example, Sweden denied a British company a contract to make magnetic-stripe cards, finding that Britain's laws failed to give Swedish data enough protection. It is this component of data protection laws—the determination whether another country's laws are adequate—that transforms data protection laws from domestic matters into international trade issues.

Within the EU, the choice was made to avoid trade disputes not by restraining the application of data protection laws, but by harmonizing—or perhaps cartelizing—data protection across Europe. The first step came with the passage in 1981 of the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. This was followed by the EU's Data Protection Directive, ratified in 1995. The preamble to the directive speaks of the importance of not permitting differences among national data protection rules to interfere with trade in goods and services across borders.[3]

From a European standpoint, "harmonization" of national laws under the Data Protection Directive would enable the creation of a free-trade zone for data within Europe. Each of the 15 EU nations would adopt some kind of data protection law within the guidelines of the directive. Regardless of the form that these national regimes ultimately take, the ratification of the directive means that there should be no more objections to free transfers of data within Europe.[4]

---

3. The European Union's Data Protection Directive is available at *http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html*.

4. See Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, D.C.: Brookings Institution Press, 1998), p. 25 (the "Directive increases the free flow of information within the European Union").

Regrettably, the directive transformed what was an intra-European trade dispute into an international one. The EU nations, having chosen to solve their own trade problem by adopting more regulation across the board (assuming for the moment meaningful compliance with the directive across Europe), rather than *less*, now find themselves at a competitive disadvantage compared with nations that allow the use of data with less regulation. This is not an unfamiliar situation; for example, European nations are also at a disadvantage because of their more tightly regulated labor markets. The directive stipulates that an EU nation may apply its data protection law to any data collector that collects or processes information within any EU state.[5] Because the substance of the directive permits a determination of the *adequacy* of the legal regimes of other nations, the new data protection regime across Europe looms as a trade barrier between the U.S. and Europe.

The Adequacy Determination. Specifically, Article 25 of the Data Protection Directive prohibits the transfer of electronic information to non–EU countries ("third countries") that do not provide an "adequate level of protection."[6] Article 26 does suggest some exemptions and exceptions that allow information to be sent across borders even in a case of "inadequate" regulatory protections, such as the consent of the subject of the information, or protections built into the contract between the subject and the data collector.

Since the traditional American approach to privacy problems is far less regulatory than the European approach, it is likely that in some contexts EU officials will see U.S. protection as inadequate; in reality, the difference in protections reflects fundamental differences between U.S. and European ideas about business and the free flow of information.

It is the determination of "adequacy" that transforms the privacy question from a concern over compliance with local laws in Europe to an international trade issue. Ordinarily, a country's protections for its citizens stop at its own borders. A country doing business in France must comply with France's consumer protection laws; if a French citizen wants to travel from France to the United States, the French government does not undertake a determination as to the adequacy of U.S. consumer protection law or criminal law before allowing the travel. Under the Data Protection Directive, however, information about the citizens of European nations is "protected" even after it leaves the country; and unfortunately for trade, this will entail an inquiry into the "adequacy" of other nation's laws.

Perhaps the data protection laws technically do not offend traditional notions of jurisdiction. The European nation does not claim jurisdiction over the firm's behavior in another country, merely over the act of exporting certain data from the nation itself. Yet the notion of determining the "adequacy" of another country's laws is clearly a mischievous one.[7] The EU nation may be regulating behavior within its borders, but the end goal is to affect behavior beyond those

---

5. Article 4 of the Data Protection Directive stipulates that EU members may apply their national data protection laws against any data collector that "makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." See Directive 95/46/EC of the European Parliament and of the Council, October 24, 1995, from *Official Journal*, L281, November 23, 1995, p. 31.
6. *Ibid.*, at Article 25.
7. For an explanation of the factors considered in an adequacy determination, see preliminary report of the United Kingdom Data Protection Registrar, "The Eighth Data Protection Principle and Transborder Data Flows," July 1999, at *http://www.dataprotection.gov.uk/transbord.htm*.

borders, even to the extent of insisting that foreign governments pass certain laws restricting information use.

Admitting the legitimacy of such an approach invites trade war upon trade war as nations take turns standing in judgment of one another's internal regulatory regimes. Indeed, some European nations' legal regimes could be deemed inadequate to preserve the economic benefits of the free flow of information to consumers, or their labor laws could be determined to be inadequate to protect free labor markets, and so on.

Data Protection or Data Protectionism? Another reason that EU data protection laws present a trade issue is the danger that the rules adopted in Europe could effectively protect European firms from U.S.-based competition. Several factors contribute to this risk.

The standards of "adequacy" are not specified in the Data Protection Directive—leaving the various European nations with broad discretion as to how to enforce their data protection laws. In some nations, like Greece and Italy, regulatory enforcement is very lax. Even in the United Kingdom, it is believed that many companies do not comply with the new data protection law.[8] There is evidence that data protection rules are not being enforced against Web sites; U.S. companies are far ahead of European ones in posting privacy policies online.[9] Any U.S. firm that wishes to begin to process employee or customer data in Europe faces months of delay in winning approval from data protection regulators.[10] For example, Spanish officials used data protection laws to niggle with Microsoft over the colors and typefaces in Windows 98.[11] Yet it is far from clear that this level of compliance is being demanded of their foreign competitors.

Further complicating the issue, the principles underlying data protection laws are grossly overbroad; for example, in theory, a businessman who accepts a business card from a client in Rome and then decides to travel to New York must provide the client with some kind of explicit notice and opt-out before leaving the country. If the directive is taken literally, merely taking a laptop on an airplane is a tremendously controversial act.[12] In practice, of course, it would be absurd to prosecute the travelers in such cases. But this means that there will be far more violations of data protection rules than cases worth prosecuting; enforcement can be arbitrary.

All of this will tempt European officials to insulate European-based firms from competition by focusing enforcement efforts on firms from outside the EU. At least, while negotiations continue regarding financial services, there has been no broad effort to enforce data protection laws against U.S.-based financial services companies.[13]

European authorities also should recognize that the *de facto* focus on U.S. or other foreign firms would harm European consumers by limiting choice and competition. It harms European businesses that deal with U.S. companies as well.[14] Both parties to a free trade agreement

8. "UK Firms Unprepared for New Data Regulation," *The Financial News*, October 8, 2001.
9. Joris Evers, "U.S. Beats Europe in Online Privacy Protection," *InfoWorld.com*, January 24, 2000.
10. Ellen Messmer, "EU Data-Privacy Laws Bog Down U.S. Firms: Bureaucratic Process Can Delay Application Projects by Months," *Network World*, December 17, 2001.
11. *Ibid.*
12. Swire and Litan, *None of Your Business*, pp. 46, 70.
13. Steve Jarvis, "U.S., EU Still Don't Agree on Data Handling," *Marketing News*, August 13, 2001.

benefit from the free trade. While free trade regimes such as the WTO have been established to address the threat of such regulatory protectionism, the agreements leave individual national governments with considerable leeway to take protectionist measures so long as the law can be justified by some colorable excuse. Thus, some European restraints on the import of beef grown with certain hormones or restraints on television programming with certain cultural content remain in place. Data protection rules could turn out to be another such instance.

The free flow of consumer information within the U.S. economy has made the United States one of the world's most powerful service economies. To abandon this general principle would be to sacrifice one of America's foremost competitive advantages in the global economy. Competition between nations' regulatory regimes provides a check on over-regulation worldwide.

APPLICABLE PRINCIPLES IN EXISTING AGREEMENTS

Privacy policy generally should not be considered in isolation from trade policy. Trade negotiators should be aware of how addressing one set of principles affects the other. Several existing trade agreements incorporate relevant principles.

THE "SAFE HARBOR" AGREEMENT

Europe's Data Protection Directive officially took effect on October 25, 1998. The EU and the U.S. Department of Commerce had initiated negotiations to set out clearly how U.S. firms doing business in Europe could satisfy the terms of the directive, given that the United States did not take a top-down regulatory approach to privacy. The documents resulting from these negotiations provide U.S. firms with a "safe harbor" from prosecution under the terms of the directive[15]—assuming, of course, that authorities administering the various national data protection regimes also accept the safe harbor principles.

The substance of the safe harbor provision is a restatement of the vague principles of data protection—such as notice, choice, and access. As a legal document, it provides little guidance either to EU national governments or to U.S. firms on exactly what measures must be taken to avoid liability. And since some individual EU groups[16] and member nations at times have refused to accept the principles like safe harbor negotiated between the EU and the United States, it remains to be seen exactly how "safe" a safe harbor will be.

In July 2001, the European Commission approved the safe harbor exception; but just before the commission's ruling, in a non-binding vote, the European Parliament rejected the deal. Reportedly, its main criticism was the absence of a government forum that would enable European residents to settle privacy disputes with U.S. companies. The Parliament planned to review the effectiveness of the safe harbor deal in 2002, after it had been in effect for a year.[17]

---

14. Thus, the Confederation of British Industry has called for more relaxed rules on the transfer of data between Europe and jurisdictions such as the United States. See "UK Bosses Want Data Policy Review," Newswire (VNU), September 28, 2001.
15. "Welcome to the Safe Harbor" and other Safe Harbor documents are available at *http://www.export.gov/safeharbor/sh_documents.html*.
16. An EU Working Party states that the implementation of "safe harbors" does not provide adequate guarantees. See *Working Party on the Protection of Individuals with Regard to the Processing of Personal Data*, Opinion 7/99.
17. Patrick Thibodeau, "U.S. 'Safe Harbor' Rules Questioned," *InfoWorld Daily News*, September 13, 2000.

Sweden still considers the safe harbor inadequate;[18]and although the safe harbor agreement puts enforcement in the hands of the FTC and private parties in the United States, the European Commission has declared that a significant number of signatories to the safe harbor have not complied to their satisfaction.[19] Because of this continued uncertainty and the accord's vagueness, companies have been slow to take advantage of the safe harbor provision, with only about 130 signing the accord as of November 2001.[20] Those that do sign must still enter negotiations with each EU nation's data protection authorities if they wish to know more exactly what is expected of them.

As an alternative or in addition to the safe harbor, companies may enter into negotiations with national data protection authorities to set out contract terms under which information about consumers and the company's employees will be protected. This contractual approach has the advantage of offering more precise terminology than the vague concepts of the safe harbor, but it imposes a tremendous burden on the individual firms involved in the negotiations. Essentially, they must negotiate under duress, with the national authorities holding over their heads the threat of exclusion from commerce.

To make matters worse, the European Commission has become involved in the business of drawing up "model contracts" for this purpose—an unacceptable level of regulatory micromanagement. Furthermore, in the area of marketing, the policy announced by the commission in the spring of 2000 regrettably reverses the usual presumption of liability, starting with the assumption that it is up to a marketing company to prove that it is not violating the data protection rules rather than up to the regulator to prove a violation. This proposal is not consistent with the rule of law, and it threatens massive trade disruptions in normal business activities.[21]

Because the safe harbor agreements did not cover financial services firms, the EU also proposed to have financial services firms satisfy data protection requirements by signing contracts guaranteeing privacy protection for data exported from Europe. In March 2001, officials from the Treasury Department and the Commerce Department rejected this as unworkable. The Bush Administration found that the terms of the model contracts would "impose unduly burdensome requirements that are incompatible with real-world operations."[22] The Administration also noted the underlying trade problem: that the EU was "trying to impose laws beyond its own frontier."[23] The United States asked that the implementation of data protection rules to financial services be delayed, but the EU rejected this proposal in May 2001.[24] In January 2002, negotiations between the EU and the United States on the financial services industry were resumed.

18. Michael Fjetland, "Global Commerce and the Privacy Clash," *Records Management Quarterly*, January 1, 2002.
19. "Some U.S. Safe Harbor Firms Fail to Meet E.U. Transparency Rules," *Europe Drug & Device Report*, February 25, 2002.
20. Hemphill, "Information Technology and Innovation Policy in the Bush Era."
21. Direct Market Association, "DMA Disappointed at European Commission's Proposal," press release, April 3, 2001.
22. Hemphill, "Information Technology and Innovation Policy in the Bush Era."
23. *Ibid.*
24. *Ibid.*

THE "MOST FAVOURED NATION" PRINCIPLE

The General Agreement on Trade in Services (GATS). One of the World Trade Organization's most important agreements is the General Agreement on Trade in Services, which came into force in January 1995. Essentially, the GATS is a multilateral agreement affecting international trade in such services as banking, insurance, satellite communications, and telephony.[25]

An important principle established in the GATS is "Most-Favoured-Nation [MFN] Treatment."[26] WTO members must give the service suppliers of other members "treatment no less favourable than that accorded to like services and suppliers of any other country." Before the agreement went into force, members were permitted to list exemptions. These Article II exemptions are subject to review and not intended to last longer than 10 years.[27] However, data protection rules have their own general exemption in Article XIV of the GATS:

> [N]othing in this agreement shall be construed to prevent the adoption of enforcement by any Member of measures… (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: …(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality or individual records and accounts.[28]

Under these provisions, some have raised the possibility that, if two different outside countries are bidding to provide services within an EU nation, the refusal to award the contract to one bidder on data protection grounds would violate the MFN clause of GATS.[29] Because data protection is exempted under Article XIV, this is perhaps unlikely so long as the rules are not applied in a discriminatory manner, but it remains to be seen to what extent this will occur.

Currently, a new GATS agreement is being negotiated. So far, the interpretation of the non-discrimination provisions of the MFN clause and the exception for data protection have not become issues in the negotiations.

From the standpoint of furthering competition in services—especially financial services—in Europe from U.S. firms, the exemption should be revisited. The Article XIV exemption was negotiated before the EU's Data Protection Directive was finalized. In 1994, when the GATS agreement was worked out, data protection laws were causing notorious trade disputes between different European nations; few anticipated this would much affect the activities of U.S. firms in Europe. But the Europe-wide Data Protection Directive changed this assessment. Now the Article XIV exemption for data protection has a more obvious potential impact on U.S. firms.

---

25. General Agreement on Trade in Services, Annex 1B. For more information, see World Trade Organization, "The GATS: Objectives, Coverage, and Disciplines," at *http://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm* (August 14, 2001).
26. General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization, Annex IB, April 15, 1994 (cited hereafter as GATS).
27. WTO, "The GATS: Objectives, Coverage, and Disciplines."
28. GATS, pp. 294–295, at *http://www.wto.org/english/docs_e/legal_e/26-gats.pdf*.
29. See Swire and Litan, *None of Your Business*, p. 190.

At the very least, it would be appropriate to ask why national data protection rules should not be viewed as Article II exemptions (subject to review) rather than general exemptions under Article XIV. Unlike the other Article XIV exemptions, at least where data protection rules affect the use of information by legitimate businesses, data protection has little or nothing to do with a sovereign state's traditional prerogative to protect public morals, health, and safety, or with preventing fraud.

The General Agreement on Tariffs and Trade (GATT). Whereas the GATT applies to trade goods generally, the GATS essentially is the subset of rules that apply to services. The GATT also contains an MFN clause.[30] It contains no exemption, however, for data protection laws. This raises the possibility that challenging data protection laws would be easier for a company sending information across borders in association with the trade in goods than it would be for a company sending data across borders in association with a trade in services.

SHOULD DATA PROTECTION BE ON THE WTO'S AGENDA?

Like any extremely vague regulation, data protection rules could easily be applied in a discriminatory manner that reduces competition from foreign businesses operating in an EU nation. At an even more basic level, a restriction on the movement of information across borders clearly is a barrier to trade. The question remains, however: What is the proper forum for addressing this type of trade issue?

Several commentators have considered the possibility of raising privacy and data protection at the WTO,[31] but raising the issue at the WTO could be a double-edged sword. Note, first, that there are two ways to bring data protection issues to the attention of the WTO. One way is to challenge EU nations' decisions to exclude U.S. firms on data protection grounds under the WTO's existing nondiscrimination principles. Clinton Administration officials had stated their willingness to do so if European nations began to exclude U.S. firms on data protection grounds, saying that "if we have to go to the WTO, we will."[32] Such a step might indeed be desirable and would further the debate about whether, as some EU officials have urged, the world really needs to concede to Europe's insistence on data "protection." The harder question is whether data protection should be an agenda item at future WTO talks.

Adding privacy to the WTO agenda opens the possibility of developing new GATT or GATS principles that specifically address the data protection issue. Peter Swire, former White House Chief Counselor for Privacy, and Robert Litan, Brookings Institution Chair of Economic Studies, warn that the WTO may be an inappropriate forum for "complex issues such as privacy protection that are only modestly related to free trade and protectionism."[33] This argument is weak; privacy is certainly complicated, but data protection laws are directly related to free trade because they restrain the free movement of information across borders. In this respect, privacy is much more obviously a trade issue than is, say, the environment.

---

30. Kevin Bloss, "Raising or Razing the E-Curtain?: The EU Directive on the Protection of Personal Data," *Minnesota Journal of Global Trade*, Vol. 9 (2000), p. 645.
31. See, for example, Lukas, "Safe Harbor or Stormy Waters?" pp. 7–11.
32. Swire and Litan, *None of Your Business*, p. 189.
33. *Ibid.*, p. 196.

Swire and Litan also point out, however, that the WTO may be dominated by EU officials who would prefer a more regulatory approach than that taken by the United States. Indeed, EU officials have supported the inclusion of e-commerce in the WTO's agenda for treaty talks, and one of their interests would be to further the cause of more data protection regulation worldwide.[34]

Principles developed at the WTO that challenge the EU justifications for limiting the flow of information across borders might be good for free trade. But then again, the new principles might be bad for trade and competition, creating exemptions from free trade principles (like the existing exemption in GATS) that would bring to a premature end the debate about whether data protection rules are a justifiable limit on free trade. Another temptation would be to accede to a global privacy regime to defuse the potential for protectionism with national data protection rules[35]—when substantive questions exist as to whether following the EU privacy model would cause more harm than good for consumers and national economies.

At this point, it is still unlikely that data protection will become an issue at WTO negotiations, given the difficult nature of many of the other items on its agenda, such as agricultural quotas. Nevertheless, privacy eventually will arrive on the international trade stage either as an agenda item for a meeting or in a dispute resolution forum. When it does, U.S. negotiators should stand firm to preserve the freedom of trade when facing pressure to impose stricter data protection regulations.

THE REAL DEBATE FOR TRADE NEGOTIATIONS

The simple fact that Europe's data protection rules are different from those of the United States might lead one to the view that the main direction in trade negotiations should be toward more *uniform* rules. But treating this as the main issue assumes that objections to uniform rules based in considerations of national sovereignty or the need for competition between different regulatory regimes are unimportant—an assumption that the foregoing analysis shows is unwarranted. It also assumes that it does not make much difference which set of rules is adopted so long as the rules are uniform.

In reality, however, this latter assumption is also unwarranted. In fact, for both consumers and business, the U.S. regime, which favors the freedom of information, is superior. If the uniform rules follow the European model, the benefits of uniformity are likely to be outweighed by the costs of over-regulation.

The debate about privacy regulation has often presented a false dichotomy between morality and economics. In the context of trade negotiations, the dichotomy will likely be presented, initially at least, as free trade vs. human rights or consumer protection. (While the WTO exempts laws that protect "human rights" from being struck down as trade barriers, there has been little or no discussion of how this might affect the privacy debate.)

If the debate is allowed to be framed in this manner, free trade could be the loser—undeservedly so, because data protection regulations should not be serious contenders as "human

34. Heinz Hauser and Sacha Wunsch–Vincent, "A Call for a WTO E-Commerce Initiative," *International Journal of Communications Law and Policy*, Vol. 6 (Winter 2000/2001), pp. 1, 30, n. 21.

35. See, for example, Paul Raines, "Global E-Commerce Privacy Should Be on the WTO Agenda," *ebiz Chronicle.com, Backgrounder*, July 2, 2001.

rights" or "consumer protection" rules, as those terms are generally used. Indeed, the free movement of information across borders has a stronger claim to recognition as a human right—and offers a net benefit to consumers and economies.

THE "RIGHT" TO DATA PROTECTION VS. FREEDOM OF INFORMATION

The basic rule of democratic societies is that people are free to communicate truthful information about other people and events to one another. If that default rule were abandoned, it would have the effect of outlawing much ordinary conversation as well as the practice of journalism. In the United States, this principle is recognized and protected by the First Amendment to the Constitution, which protects free speech. The free movement of information has been the rule, with restrictions to protect privacy confined to special areas like medicine.

A review of U.S. common law cases shows that privacy lawsuits are confined to very narrow ground by free speech principles.[36] Similarly, other restrictions on the use of information—copyright law, patent law, and defamation—are likewise hemmed in by free speech principles. One cannot copyright a fact or an idea. The debate is free speech versus privacy, not morality versus economics.

This core tension cannot be alleviated by confining privacy rules to regulate businesses' use of information alone. Persons learning about others in a business context are still human beings; there is no reason to suppose that Everyman sheds his rights when he puts on a suit to go to work. Journalists certainly do not. As Justice Antonin Scalia has pointed out, we may care more about our decision to buy a house than about the war in Bosnia. The framers of the Constitution made no distinction between commercial speech and other speech; indeed, to them, free speech was important as an aspect of property rights.[37] The United States Supreme Court has increased the protection for commercial speech over the years and ought to move further still in that direction.[38]

Europe's data protection regime has at its root principles that are fundamentally hostile to the free exchange of information. In essence, it establishes a series of rules for processing all kinds of personal information that give the "data subject" (the person the data describes) a right to control facts and opinions about himself uttered by others, which must be regulated. As a basic principle, this is dangerous. One can immediately think of a million situations in which one's attempt to learn about others without the other's consent is perfectly legitimate. Essentially, the premise behind the Data Protection Directive is not compatible with ordinary human life.

Accordingly, the directive itself has come to be riddled with exemptions, starting with an exemption allowing one to keep the addresses of friends for household purposes. Another trifling exemption explains that nations may recognize free speech principles to allow journalists to function. A rather strained interpretation of the directive was required to allow switching information to be relayed through the phone network.

---

36. For a more detailed history of U.S. common law, see Solveig Singleton, "Privacy Versus the First Amendment: A Skeptical Approach," *Fordham Intellectual Property, Media & Entertainment Law Journal*, Vol. XI (Autumn 2000), p. 97.
37. See Daniel E. Troy, "Advertising: Not 'Low Value' Speech," *Yale Journal on Regulation*, Winter 1999, p. 97.
38. *Ibid.*

The exemptions are not bad things; there should be even more of them. But a morally superior rule would favor freedom, with narrow rules to restrict information when a need has been proven beyond doubt—for example, against perpetrators of fraud.

The weakness of data protection as a "human right" is perhaps best seen when it is compared with other human rights. Take, for example, the right that confessions not be obtained by torture. Observing this rule does not disturb ordinary human activity in any way, and there is no need for exemptions to it. Indeed, the thought of exemptions to it is horrifying. Data protection simply is not in that league of "rights."

CONSUMER PROTECTION VS. FREE TRADE IN INFORMATION

In a trade context, data protection might also be defended as consumer protection. The difficulty with that position is that it is difficult to see from what exactly the data protection rules would protect consumers. One important impact of the directive, after all the exemptions are done, is on direct marketing to consumers. Arguably, then, it protects consumers from coupons and catalog mailings. Yet studies show that consumers reap many benefits from advertising—from finding out about new products to vigorous price and quality competition among businesses seeking consumers' dollars. Economist George Stigler has observed that advertising is "an immensely powerful instrument for the elimination of ignorance."[39]

In short, advertising serves as a spur to competition, helping consumers to identify new entrants into the market, new products, and the best deals. Consumers benefit from information-sharing more generally in other ways, too.

Adopting European-style regulation would mean that many of these benefits would never be realized. In the United States, cost savings from information-sharing in financial services alone have been estimated at $17 billion per year for the customers of just one group of companies. The savings would be larger still for the entire financial services industry.[40] A study of the apparel industry in the United States estimates that an "opt-in" rule would effectively impose a $1 billion tax on catalogue and Internet clothing sales as businesses passed on a cost increase of from 3.5 percent to 11 percent.[41]

The impact of new law on innovation and future ventures that might use consumer information in unforeseen beneficial ways should not be underestimated. Had opt-in (or even opt-out) been the rule in the late 19th century, for example, credit reporting could never have been invented. Most people even today would have to depend on the good will of their local storekeepers or bankers to get credit.

One real danger from which consumers need to be protected is fraud and identity theft; but this is a security issue, not a privacy issue. In many respects, good security requires more investigation and tracking, not less; and in that sense, strict data protection rules can make a system less, not more, secure. For example, under an opt-in or even an opt-out regime, address authentication and verification services used by e-merchants like Amazon.com would

39. George Stigler, "The Economics of Information," *Journal of Political Economy*, Vol. 69 (1961), pp. 213, 220.

40. Ernst & Young for the Financial Services Roundtable, "Customer Benefits from Current Information-Sharing by Financial Services Companies," December 2000, at *http://www.fsround.org/PDFs/custbenefits.PDF.*

41. Michael A. Turner, "The Impact of Data Restrictions on Consumer Distance Shopping," Information Services Executive Council, white paper conducted for the Privacy Leadership Initiative, Spring 2001, at *http://www.understandingprivacy.org*.

be much less effective in catching errors and attempted fraud. Under data protection, attempts to develop super-secure biometric identifiers like fingerprint or retinal scans could be held back.

In any case, fraud and identity theft are already illegal in the United States. Where consumers need more help is in the area of enforcement. New and more effective enforcement institutions could be developed to address these harms without penalizing the economy.[42]

Nevertheless, it is important for U.S. trade negotiators to understand Europeans' emotional sensitivity on this issue. Historically, the impulse behind data protection is the memory of the horrors of the misuse of census data to track down Jews, gays, gypsies, and other "undesirables." Data protection came to be seen as especially important as centralized welfare states grew up in Sweden and elsewhere.

This impulse is understandable—a concern for the misuse of information by government is shared by many in the United States. The difficulty is that data protection is not a rational outcome of this impulse. The reason: Data protection rules exempt government's processing of information for most governmental purposes. In this respect, the U.S. constitutional tradition gives Americans far more protection from real threats to privacy than most Europeans enjoy. The San Diego judge who invalidated 250 tickets issued by "red light" cameras, which were set up to guarantee unfair tickets, is just one example.

GUIDELINES FOR TRADE NEGOTIATORS

U.S. negotiators in trade talks would do well to keep in mind these points when discussing data protection:

- **The free movement of consumer information across borders is a key part of a free economy and a free society.** There is no need for U.S. businesses or government representatives to "apologize" for the U.S. approach to privacy. In the United States, the presumption against commercial regulation—allowing privacy regulation to trump the free movement of information only in exceptional cases—is morally and economically the superior position. Freedom of information has a far more respectable philosophical pedigree than novel principles of "data protection." Studies show that the costs of more privacy regulation to consumers are likely to far exceed the benefits.
- **European consumers and businesses would also benefit from less regulation.** Companies from the United States enter European markets to provide services to European consumers and businesses. They increase competition in European markets. Despite the recent economic downturn, the United States is still the world's greatest service economy, and the freedom to innovate with new uses of information has a great deal to do with that. Europe would do well to follow the U.S. example.

42. Representative James Leach, "Identity Theft Vexes Lenders, Consumers," *Mortgage Servicing News*, November 2000, p. 4. ("Despite [the] profusion of Federal and State statutory authority…there is little evidence that law enforcement agencies have made combating this crime a priority. A recurring theme at least week's hearing was the difficulties encountered by victims of identity theft and the financial institutions that bear the losses in obtaining redress, either because financial thresholds established by prosecutors' offices have not been met or because resources are simply being directed elsewhere.") See Jackie Hallifax, "Task Force Grapples with Privacy Issues in Technology Age," Associated Press State and Local Wire service, December 15, 2000 (outlining better enforcement methods for identity theft).

- **The focus of privacy efforts should be on the threats to privacy posed by government over-regulation.** Whether in the United States or Europe, governments have unique police powers that the private sector lacks, and thus pose a greater risk to misuse of information. In the United States, the Constitution, particularly the Fourth Amendment, provides significant protection for privacy where it is most threatened: in criminal cases. By contrast, the Data Protection Directive actually exempts criminal cases from the scope of its privacy protections.
- **The facts about European data protection laws should be sought from firms and individuals doing business within the EU**. Numerous key questions remain about the impact of data protection rules in European nations. What has the cost of these rules been? What has the effect of the rules been on small businesses and new business ventures? On the detection of fraud and the assessment of credit risk? How are the laws enforced? Official European sources may not be the best source for this information. The other side of the story should be sought from European businesses. Because data protection is such a radical departure from the tradition of freedom of information, the burden of proof should be on advocates of the regulation to show that it would do more good than harm.
- **U.S. trade agreements should not adopt data protection as a means of satisfying EU requirements.** This would set a terrible precedent for future trade disputes concerning labor and environmental regulation. It would also set a bad precedent for U.S. economic relations with Canada, another country that has adopted data protection laws similar to those in Europe—but without (so far) engaging in any inquiry into the adequacy of protections for Canadian data in the U.S. Moreover, a diet of data protection harms the emergence of innovative businesses and new consumer services, especially in developing countries.
- **U.S. officials should be aware of discussions of data protection in other areas of the world.** As in the United States, European officials are making the case for more restrictive data protection rules in other countries, particularly Asian countries. The adoption of tough data protection rules everywhere else would give the United States a competitive advantage from an economic standpoint, but we might well benefit more from the increased world economic growth that would be enabled by less regulation worldwide.
- **In the area of financial services, the privacy provisions of the Gramm–Leach–Bliley Act are more than sufficient.** In ongoing negotiations, EU officials may take the position that current privacy regulations for financial services, which allow consumers to opt out of inclusion in many marketing lists, are "inadequate." Many privacy advocates prefer an "opt-in" system. But consumers may find an opt-in system even more intrusive, and its costs are enormous. U.S. West, one of the few businesses in the United States to operate under a European-style opt-in system, found it cost $30 per customer contacted to obtain a consent and required an average of 4.8 calls to each household before the company reached an adult who could grant consent.[43] U.S. trade representatives should not accept the view that opt-in regulation for financial services would benefit consumers.

43. Coalition for Sensible Public Records Access, *The Limits of Opt-In*, at *http://www.cspra.org/* (February 18, 2002).

CONCLUSION

Even in Europe, data protection dates back only as far as the 1970s, and at that time was intended mainly as a restraint on government information processing. As compared to the strong legal tradition of the freedom of information and the proven benefits of free trade, data protection has dubious justifications.

The foregoing analysis shows that European insistence on judging the "adequacy" of U.S. law before allowing trade in information to proceed is incompatible with the ordinary exercise of national sovereignty. "Data protection" laws can be expected to operate as trade barriers. The "safe harbor" approach to this problem has not eliminated this problem, both because of restrictive European interpretations of its principles and because its principles themselves are vague and overly regulatory. The "model contract" approach taken so far for financial services has likewise not succeeded well, again because the contracts supported so far by European officials do not seem to recognize fundamental business realities.

The Bush Administration has done the right thing so far in rejecting this approach. European officials who come to discuss information policy with U.S. representatives should realize that they have as much to learn as they have to teach.

—Solveig Singleton is a lawyer and senior analyst with the Competitive Enterprise Institute's Project on Technology and Innovation.