2006

Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization

Virginia Boyd

Recommended Citation

Link to publisher version (DOI)
https://doi.org/10.15779/Z381360

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Journal of International Law by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.
Financial Privacy in the United States and the European Union:
A Path to Transatlantic Regulatory Harmonization

By
Virginia Boyd*

I.
INTRODUCTION

Information has been described as the “cornerstone of a democratic society and market economy,”¹ and enhanced technologies for using personal data have arguably transformed financial services into an “information industry.”² Walter Wriston, former chairman of Citicorp, asserted that “information standards” have replaced money in global financial markets.³

Information today is fundamentally global. The technologies that carry it ignore national borders. Multinational corporations and consortiums of organizations that share data dot the globe. In the case of the Internet, multinational banking networks..., credit and financial services networks..., and stock and commodities networks..., it is virtually meaningless to talk of national privacy law. What consumers and service providers alike need are common standards applicable throughout the world. Commonality does not require identical laws but rather legal regimes that, while still reflecting national contexts, are based on shared principles.⁴

The sheer technological power of the digital age, offering huge advances in the type and quality of products offered in the economic marketplace, also poses unprecedented threats to personal safety and autonomy if privacy is not adequately protected. In response to mounting privacy concerns in an era of

---

¹ FRED H. CATE, PRIVACY IN PERSPECTIVE xiv (2001) (quoting the Federal Reserve Board).
² Richard M. Kovacevich, Privacy and the Promise of Financial Modernization, 14 THE REGION 1 (2000) (Kovacevich is the former president of the Financial Services Roundtable).
escalating technology, as well as concerns that divergent standards could undermine the functioning of a Single Market, the European Council ("EC") of the European Union\(^5\) enacted a Directive in 1995\(^6\) to safeguard all personal information of its citizens. The Directive may be the world’s most ambitious and far-reaching data privacy initiative of the high-technology era.\(^7\) Significantly, it imposes restrictions on data transfers outside the EU to countries that have not been found to provide “adequate protection.” It thus creates tension between the goal of harmonizing trans-Atlantic financial regulation and the need to respect national legal regimes.\(^8\) The United States approaches privacy differently, in part due to a reluctance to enact universal privacy legislation for constitutional and historical reasons. Varying degrees of privacy legislation exist in different sectors of the US economy, largely in response to perceived dangers of abuse, and the European Union has not found that the overall level of protection in the United States meets the European standards. Because great volumes of personal information are transferred across borders daily, divergent standards could lead to the emergence of data havens and the EU’s imposition of restrictions on certain data transfers to the United States where privacy regulation has not been deemed adequate, either of which could pose significant obstacles to overseas trade.\(^9\) The levels of privacy protection provided in the United States and the European Union must be harmonized, or at least recognized as equivalent, in order to maintain the integrity of global financial markets.\(^10\)

It may be debated how the international privacy standards should be determined. It is currently unclear whether the EU’s efforts to enforce its Directive will set the global standard or whether the standard will emerge as a hybrid of the data protection practices of several large commercial countries. Some have expressed skepticism as to the feasibility of establishing a standard through international treaties,\(^11\) yet others believe that such voluntary

\(^5\) The European countries that currently belong to the EU are: Austria, Belgium, Cyprus, Czech Republic, Estonia, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.


\(^8\) Id.


\(^10\) See CATE, supra note 4, at 129.

Anchoring its data protection legislation in a fundamental human right to privacy, the EC Directive created a broad data protection framework applicable to almost all personal information held by any data controller in any sector of the economy. However, enforcement of the Directive has not been ideal for a number of reasons, including inconsistent Member State implementation. In the United States, privacy of personal information is not a fundamental or explicit Constitutional right. US privacy protection has emerged as a sectoral “skyline,” with skyscrapers (high regulation) in some areas, such as the financial and health care industries, and tenements (lower regulation) in others. Currently, federal privacy protections for consumers in the financial services sector are contained in the provisions in Title V of the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999, 15 U.S.C. §§ 6801-6809 (2006) and in the Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. §§ 1681-1681u (2006), amended by the Fair and Accurate Credit Transactions Act (FACTA) of 2003 (2006). In addition, federal statutes, including the Electronic Funds Transfer Act (EFTA), 15 U.S.C. § 1693 (2006) and the Equal Credit Opportunity Act (ECOA), 15 U.S.C. §§ 1691-1691f (2006), state law, self regulation, codes of conduct, and market mechanisms play a significant role in the actual privacy protections provided to customers of financial institutions.

This paper will outline the overall data protection standards and the enforcement mechanisms applicable to the financial services sectors in the United States and the EU with a view toward identifying the disparities in approaches and in functional privacy protections. It will offer key legal modifications that would enable the US financial services sector to qualify for a sectoral adequacy decision by the European Commission. Part II will focus on the US approach to data protection, illustrating the US reliance on a theory of self regulation, harm prevention, and active enforcement in the design of its sector-based privacy system. Part III will turn to the EU’s approach to data protection, characterized most significantly by an emphasis on the concept of privacy as a fundamental human right and on stringent formal legal regulation with somewhat inconsistent enforcement.

Part IV will compare and contrast the two jurisdictions’ regulatory systems using a functional similarity analysis, considering first the content of the privacy principles applicable to financial institutions and then actual enforcement in the United States and the EU. Despite differing conceptions of privacy, it is possible that two distinct approaches could lead to functionally equivalent protections for consumers. In the United States, a mixture of self-regulatory,  

12. As Professor Fred Cate stated, referring to the international agreement providing for global harmonization of copyright laws: “It is time for a Berne Convention for privacy.” CATE, supra note 4, at 129.
federal, and state legislative systems can give rise to real protections. On the other hand, Member States’ varying implementations of the Directive may weaken its formal privacy protections, indicating that privacy in the EU is actually governed by less stringent standards than its Directive suggests. Logically, the EU should hold third countries only to those standards by which EU companies are actually required to abide. Finally, Part V will consider the Directive’s restrictions on transfers to the United States and evaluate potential modifications of US data protection law that would ensure that the US financial services sector provides “adequate protection” for personal data, indicating why such a determination is important given the current stalemate.

I conclude that, if the United States makes a few key amendments to the applicable federal laws, it would be appropriate for the EU to make a sectoral adequacy determination for financial services based on the entirety of legal and other regulatory protections afforded in that sector in the United States.

II. REGULATION OF FINANCIAL PRIVACY IN THE US

A. Historical Overview of Financial Privacy Regulation

Although the United States has been credited with inventing the concept of individual privacy with respect to government intrusions, information privacy is not explicit in the Constitution and may even run counter to the First Amendment’s protection of free information flows. Privacy is not perceived as an absolute, fundamental human right, equivalent to liberty or equality. Rather, information privacy laws are generally adopted because of a perceived need to protect against specific abuses of private personal information, risk of which must be balanced against the benefits that result from increased efficiency of information sharing. Some have described the limits of privacy protection in the United States as being shaped by the strength of the external forces of the time, such as the fear of terrorism after September 11, 2001, rather than by any intrinsic or fundamental value. The US legal tradition breeds a reluctance to regulate the private sector absent a demonstrated need, and there is generally

14. See CATE, supra note 4, at 58. The concept of privacy is often traced to Brandeis & Warren’s article, The Right to Privacy, 4 HARV. L. REV. 193 (1890). See DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306 (1989) (stating that “the United States invented the concept of a legal right to privacy”). In the public sector, the debate over invasions of privacy centers on the Fourth Amendment, in particular the idea that the zone of protected privacy is defined by both the individual’s actual, subjective expectation of privacy and the extent to which that expectation was “one that society was prepared to recognize as reasonable.” United States v. Katz, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

15. CATE, supra note 4, at 56-57. In Whalen v. Roe, 429 U.S. 589 (1977), the Supreme Court applied intermediate scrutiny to a privacy-based challenge because strict scrutiny was reserved for laws touching on ‘fundamental’ interests.

greater concern about government than private sector excesses.\textsuperscript{17} As Professor Fred Cate stated, "Regulation of privacy in the United States has focused on preventing the uses of information that harm consumers."\textsuperscript{18}

In the financial services industry, the harms arising from information sharing include increased likelihood of fraud through unauthorized collection, use or transfer of information (including, surreptitious monitoring of personal habits, profiling, identity theft, telemarketing, denying benefits based on inaccurate information), and retaining harmful information indefinitely. Against these harms must be measured the benefits of information sharing, which include expanding availability and reducing delays and costs of consumer credit, identifying and meeting consumer needs, promoting competition, enhancing customer convenience and service, targeting interested consumers, and preventing fraud. While the financial services industry has generally resisted costly privacy protection measures, there is some evidence that more stringent privacy policies can actually benefit companies because consumers value their privacy and are willing to pay for it. For this reason, the banking industry has historically adhered to voluntary standards of confidentiality.\textsuperscript{19}

Consistent with this balancing approach, US financial privacy regulation is strongest in the areas that are most likely to give rise to unauthorized uses or abuses of personal information. However, the underlying substantive ideology of privacy protection, initially codified in the 1973 "Code of Fair Information Practices,"\textsuperscript{20} is similar to the EU's fundamental principles because the United

\begin{footnotesize}
\textsuperscript{17} BARBARA S. WELLBERY, BRIDGING THE DIFFERENCE: THE SAFE HARBOR AND INFORMATION PRIVACY IN THE UNITED STATES AND THE EUROPEAN UNION 4 (2001). After the terrorist attacks of September 11, 2001, the US enacted the USA PATRIOT Act, which has caused some tension between the US and the EU with respect, for example, to the privacy of EU citizens traveling to the US. See, e.g., the Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection. See also Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC).

\textsuperscript{18} CATE, supra note 1, at 4.

\textsuperscript{19} A recent study indicates that customers who have more confidence in their financial institutions' privacy policies are substantially more likely to engage in other financial services, such as online banking. Peter Swire, Efficient Confidentiality for Privacy, Brookings—Wharton Papers on Financial Services (2003).


(1) There must be no personal data-record-keeping systems whose very existence is secret.

(2) There must be a way for an individual to find out what information about him is in a record and how it is used.

(3) There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

(4) There must be away for an individual to correct or amend a record of identifiable information about him.

(5) Any organization creating, maintaining, using or disseminating records of identifiable
\end{footnotesize}
States adopted the 1980 Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, on which the EU privacy principles are also based. Most recently, in 1998, the Federal Trade Commission (FTC) articulated the core principles of US privacy as notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. Notice has been interpreted as the “most fundamental principle” because, “without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.”

While US federal privacy law exists in several areas in addition to financial services, it does not exist comprehensively. Certain information sharing between financial institutions is regulated under the Bank Secrecy Act, as amended by the USA PATRIOT Act. The insurance industry is regulated by state statutes, most of which have adopted implementing regulations and information safeguards pursuant to GLBA or the National Association of Insurance Commissioner’s (NAIC) Model Codes of 2000 or of 1982.

A series of events helped to put privacy on the Congressional agenda in 1999, pending the passage of the Gramm-Leach-Bliley Act. First, the GLBA was designed to “modernize” financial services by doing away with regulations preventing the merger of banks, stock brokerage firms, and insurance companies. New possibilities for mergers raised significant concerns that the

---

25. Section 314(b) of the USA PATRIOT Act permits financial institutions, upon providing notice to the U.S. Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. More specifically, the BSA authorizes the Treasury to require financial institutions to maintain records of personal financial transactions that “have a high degree of usefulness in criminal, tax and regulatory investigations and proceedings” and to report “suspicious transactions relevant to a possible violation of law or regulation.” Again, because this Act deals with governmental, rather than private, intrusion into customer privacy, it is outside the scope of this discussion.
new Financial Holding Companies would have access to large amounts of personal information about their customers, which they could consolidate, analyze, and sell with no restrictions.28 Internationally, the EU's 1995 Data Protection Directive, which came into effect in 1998, put pressure on lawmakers to devise a privacy system that would be deemed "adequate" by the EU. In addition, a series of high-profile cases involving marketing abuses, credit fraud and identity theft sharpened the debate and fueled consumer lobbying.29 Surveys indicated that 89% of consumers were concerned about threats to their privacy in relation to financial services.30 Finally, in Congress, much support for the Markey Amendment, creating the privacy provisions in Title V of the GLBA, came from representatives who had themselves been the victims of identity theft and other financial fraud.31 The unprecedented level of detail in financial records, combined with the possibility of comprehensive matching with other databases as a result of consolidation, indicated that self regulation alone might not be adequate to combat the rising potential for widespread abuse of personal information.32 Although compliance with consumer expectations of privacy is imperative in competitive markets, companies may have systematic incentives to overuse personal information where customers have imperfect information about privacy practices and thus will not find out about abuses.33

---

28. As pressure increased to develop a more comprehensive privacy regime in the US, more than 12% of all bills introduced in the 104th Congress included provisions on a wide range of privacy issues. CATE, supra note 4, at 131.

29. NationsBank paid civil penalties totaling $7 million to the SEC and other agencies, plus millions more in private class action settlements, over its sharing of confidential bank accountholder information with an affiliated securities firm. In addition, Minnesota Attorney General Mike Hatch sued U.S. Bank and its holding company in 1999, accusing them of having sold their customers' private, confidential information to MemberWorks, Inc., a telemarketing company, for $4 million dollars plus commissions on sales made by MemberWorks to those customers. See The Gramm-Leach-Bliley Act, Electronic Privacy Information Center, http://www.epic.org/privacy/glba (last visited March 13, 2006). See also Mark Huffman, Hard to Escape from Negative Option Trading, CONSUMERAFFAIRS.COM, Oct. 6, 2005, http://www.consumeraffairs.com/news04/2005/vertrue.html (noting, "[i]n June 1999 Minnesota Attorney General Mike Hatch sued US Bank.... The state reached a settlement, under which the bank paid $3 million and agreed to stop sharing customers' financial information to marketers of non-financial products, to give customers notice and an opportunity to "opt out" of the sale of their financial information to market financial products, and to provide certain refunds to customers charged by telemarketers who bought their account numbers").


31. Representative Joe Barton (R-TX) provided crucial and unexpected support for the Markey Amendment when his address was sold to Victoria's Secret by his credit union and, to his (and his wife's) great shock, he began to receive Victoria's Secret catalogues at his Washington home. Chris Jay Hoofnagle and Emily Honig, Victoria's Secret and Financial Privacy, Electronic Privacy Information Center (last updated January 25, 2005), http://www.epic.org/privacy/glba/victoriassecret.html (last visited March 16, 2006).

32. The 1998 FTC Report found that only 16% of banks had privacy notices or policies on their websites, and there was empirical uncertainty about how self-regulatory codes were improving practice. Swire, supra note 22, at 1284.

In addition, costs of bargaining for the desired level of privacy may be high.\textsuperscript{34}

\textbf{B. Title V of the Gramm-Leach-Bliley Act}

The core privacy protections of the GLBA’s Title V, Subtitle A are marketing disclosure, notice, choice, security, and enforcement. Starting from the premise that each financial institution has “an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information,”\textsuperscript{35} the GLBA sets out three principal requirements for financial institutions.

First, such institutions must provide customers with “clear and conspicuous” notices describing their information-sharing procedures, both at the initiation of the customer relationship and annually thereafter.\textsuperscript{36} The notices must include the financial institutions’ policies and practices of disclosing nonpublic personal information to affiliates and nonaffiliated third parties, protecting such information, and disposing of such information after the customer relationship is terminated. Second, financial institutions must develop precautions to ensure the security and confidentiality of customer records and information, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could substantially harm or inconvenience a customer. Finally, subject to certain exemptions, financial institutions may not disclose nonpublic personal information about a customer to any nonaffiliated third party unless customers are given notice and a reasonable opportunity to direct that such information not be shared ("opt out"). For example, financial institutions may not disclose customer account numbers, such as credit card numbers, to any nonaffiliated third party for marketing use. Although the GLBA does not permit customers to prevent disclosure to corporate affiliates, disclosures of certain information to affiliates may be subject to the notice and opt-out provisions of the FCRA. In addition, anti-fraud, or "pretexting," provisions in Subtitle B round out the scope of GLBA’s Title V coverage.\textsuperscript{37}

The GLBA privacy requirements apply to a broad range of “financial institutions,”\textsuperscript{38} including any bank, credit union, securities entity, insurance company, or other business that engages in activities that are “financial in

\textsuperscript{34} See \textit{id}.  
\textsuperscript{36} \textit{Id.}  
\textsuperscript{37} Title V, Subtitle B of the GLBA prohibits "pretexting," or using false, fictitious or fraudulent statements or documents, or forged, counterfeit, lost or stolen documents in order to collect customer information from a financial institution or directly from a customer. The FTC regularly reports to Congress on its enforcement actions taken pursuant to this Subtitle. However, because Subtitle B deals with fraud and other criminal activities that are dealt with by law enforcement agencies and the FTC, it is, for the most part, outside the scope of this discussion.  
\textsuperscript{38} Any institution the business of which is engaging in financial activities as described in 12 USC § 1843(k). 15 U.S.C. § 6809(3)(A) (2006).
nature” under the BHCA. The Act’s requirements are intended to protect "consumers,"—consumers are defined as people who provide nonpublic personal information to financial institutions primarily for personal, family, or household purposes—rather than corporate clients. “Nonpublic personal information” is defined as “personally identifiable financial information” obtained by the financial institution from the consumer, in connection with a transaction performed for the consumer, or otherwise. It includes consumer lists derived from nonpublic personally identifiable information, information on applications to obtain financial services, account histories, and the fact that an individual is or was a customer, as well as names, addresses, telephone numbers, and Social Security Numbers. It excludes publicly available information.

1. Notice

The GLBA notices, provided to consumers at the initiation of the relationship and annually thereafter, must contain (1) the institution’s practices with respect to disclosing nonpublic personal information to nonaffiliated third parties, including the categories of persons to whom the information is or may be disclosed, with the exceptions of disclosures under the joint marketing exception; (2) the categories of nonpublic personal information that are collected by the financial institution; (3) the policies of the institution which are intended to protect the confidentiality and security of nonpublic personal information; and (4) any disclosures required by the FCRA.

2. Choice

The GLBA adopts a basic opt-out rule, which enables customers to object to sharing personal data with nonaffiliated third parties. However, there are two main exceptions to the opt-out requirement: consumers may not prevent sharing with non-affiliates for joint marketing purposes or for certain other generally accepted statutory exceptions. Furthermore, while financial institutions must give notice before sharing with affiliates, consumers may not opt out of such sharing. The default rule of opting out rather than opting in represents a major victory for the industry. Studies show that the majority of consumers do not respond at all, and the costs of an opt-in rule would in some cases be prohibitive. Third parties that receive information pursuant to the notice and opt-out provision may reuse the information for any internal purpose,

45. The industry figure for opting out in 2001 was 5%. Swire, supra note 22, at 1267. See also Fred H. Cate & Michael E. Staten, Protecting Privacy in the New Millennium: The Fallacy of “Opt-In,” http://www.the-dma.org/isec/optin.shtml (last visited Apr. 27, 2005).
including marketing. Institutions are not required to monitor third party reuse of information. There is a blanket prohibition on disclosures of personal account numbers or other access numbers to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

i. Joint Marketing Exception

In the context of nonaffiliate sharing, the "joint marketing exception" allows financial institutions to share personal information with a partner without providing the customer with notice or choice so that partner may perform "services for or functions on behalf of" the financial institution. These services may include marketing of the financial institution's own products or services or those offered pursuant to joint agreements between two or more financial institutions subject to GLBA. However, in order to qualify, the financial institution must (a) fully disclose to the customer that it is providing such information to a third party and (b) enter into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information. Some federal agency guidelines pursuant to this exception also require the contract with a third party to prohibit the third party from disclosing or using the information for any purpose other than that for which the bank or thrift disclosed the information. For example, the banking agencies' Privacy Rule limits redisclosure and reuse of information disclosed under a GLBA joint marketing exception. Under that rule, the third party may disclose and use the information pursuant to another GLBA exception in the ordinary course of business, but it may only use it to carry out the activity covered by the exception under which it received the information. Finally, the GLBA precludes recipients from sharing non-public information pursuant to a chain of third-party joint marketing agreements.

ii. Statutory Exceptions

The GLBA permits disclosure of nonpublic personal information without providing notice or choice if one of eight conditions is met. These statutory exceptions are reasonably well-accepted by all the stake holders in the privacy

46. See Final Privacy Rule of the Banking Agencies, 65 Fed. Reg. 35,162 (June 1, 2000).
49. Id.
debate.\textsuperscript{53} One such exception is that transfers may be carried out without notice as "necessary to effect, administer, or enforce" a transaction requested or authorized by the consumer.\textsuperscript{54} The requirement of necessity has been interpreted broadly to encompass situations where disclosure is either required or is "appropriate" to enforce the right of the financial institution or whoever is responsible for carrying out the transaction. Activities considered "necessary" include: engaging in related business, servicing related claims, providing records of the transaction, and fulfilling the consumer's insurance requests.\textsuperscript{55} Notice is not required if the consumer consents or if information sharing is necessary to protect the confidentiality or security of the financial institution's records (that is, to prevent fraud, unauthorized transactions, or other claims that could give rise to liability). In addition, financial institutions may transfer nonpublic personal information to certain regulators, such as insurance rate advisory organizations, attorneys, accountants, and auditors. Disclosures permitted or required under other laws, including disclosures made to a Credit Reporting Agency (CRA) under the FCRA, to law enforcement agencies, to self-regulatory organizations, or for an investigation of a matter related to public safety also fall under the exception to the notice and opt-out requirements. Finally, disclosures are permitted in connection with the sale of a business unit or in the context of a governmental investigation.\textsuperscript{56}

A third party that receives nonpublic personal information pursuant to one of the statutory exceptions may disclose the information to its affiliates or to affiliates of the financial institution from which the information was received. It may also use the information and disclose it to nonaffiliates under one of the statutory exceptions. The third party's affiliates may only disclose and use the information to the extent permissible for the original third party. The same general rules concerning limits on reuse and disclosure apply to non-financial third parties that receive information from financial institutions.\textsuperscript{57} However, there may be difficulties concerning enforcement against such non-financial institutions from a practical point of view.

The GLBA does not provide individuals with the right to access data about themselves in order to contest that data's accuracy and completeness, but certain access rights may be guaranteed under the FCRA. However, a financial institution must disclose to a consumer the categories of nonpublic personal information shared and the categories of affiliates and nonaffiliated third parties with whom it is/was shared.

\textbf{3. Security}

The notion of "security" under the GLBA requires that financial institutions

\textsuperscript{53} Swire, \textit{supra} note 22, at 1268.
\textsuperscript{55} See 16 C.F.R 313.14.
\textsuperscript{57} 65 Fed. Reg. 35,162, \textit{supra} note 46.
implement managerial and technical measures to protect against loss and unauthorized access, destruction, use, or disclosure of data. The GLBA charges the agencies responsible for enforcing its provisions with establishing appropriate standards "(1) to insure [sic] the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."  

For example, the Securities and Exchange Commission ("SEC") and Commodity Futures Trading Commission (CFTC) require the institutions they oversee to adopt policies and procedures implementing these safeguards but do not prescribe specific procedures or policies. While it does offer suggestions for compliance, the SEC believes that it is more appropriate for each institution to tailor its procedures to its own system of information gathering and the needs of its own customers. The Federal Trade Commission (FTC), on the other hand, issued a Safeguards Rule in 2002 and is active in enforcing it.  

4. Enforcement

Ensuring financial institutions' compliance with GLBA, Title V, Subtitle A, is assigned to the five federal banking agencies, as well as to the SEC and the CFTC, with residual oversight power granted to the FTC. These agencies take enforcement actions pursuant to their regulations and guidelines. As in other areas of financial regulation, many agencies follow a highly self-regulatory approach, allowing firms to devise their own specific practices, and oversight generally entails ensuring that the safeguards provided are adequate. The GLBA also calls upon state insurance authorities to adopt implementing regulations and to enforce its provisions. There is no private right of action for consumers to claim damages resulting from privacy violations.

Enforcement of financial privacy regulation under the GLBA is complex because eight federal regulators must coordinate similar regulations implementing the GLBA's disclosure-related requirements and establishing safeguarding standards. For holding companies containing different financial

59. CCH Business and Finance Group, 1 FINANCIAL PRIVACY LAW GUIDE (2001), ¶ 3041.
61. The Federal Reserve Board of Governors ("FRB"), the Office of Thrift Supervision ("OTS"), the National Credit Union Administration ("NCUA"), the Federal Deposit Insurance Corporation ("FDIC"), and the Comptroller of the Currency ("OCC").
63. On June 1, 2000, the federal banking regulators issued final regulations implementing the privacy provisions of the GLBA. They are codified at 12 C.F.R pt. 40 (OCC); 12 C.F.R pt. 216 (FRB); 12 C.F.R pt. 332 (FDIC); 12 C.F.R pt. 716 (NCUA); 12 C.F.R pt. 573 (OTS). See 65 Fed. Reg. 35,162, supra note 46. Similar regulations for the remaining enforcement agencies are codified at 16 C.F.R pt. 313 (FTC); 17 C.F.R pt. 248 (SEC); 17 C.F.R pt. 160 (CFTC).
services companies under the jurisdiction of multiple regulators, oversight by multiple federal regulators could be problematic. The regulators may deploy the full powers that they use in other enforcement actions, and the FTC may use its powers to enforce against unfair or deceptive trading practices committed by financial institutions not subject to oversight by one of the other agencies.

Finally, a layer of state regulation and enforcement that is more stringent than GLBA may overlay the federal regulation. The GLBA’s privacy provisions generally preempt state law to the extent that state law is inconsistent with those provisions. However, to the extent that state laws afford greater privacy protection, they are deemed not inconsistent with the GLBA. In fact, many states do have stronger privacy protections, including opt-in regimes. The FTC, which has authority to make preemption determinations under the statute, has held that state opt-in requirements are not preempted by the GLBA because they provide greater consumer protection. The GLBA’s preemption provision allowing for stricter state regulation, known as the Sarbanes Amendment, was hailed by Minnesota Attorney General Mike Hatch as the “best hope to secure protections for consumers.”

More stringent regulation by large states may raise national compliance costs for firms, and stricter state laws may provide private rights of action where the GLBA does not.

C. The Fair Credit Reporting Act

The FCRA also applies to personal information and, in particular, to the information contained in consumer reports. Consumer reports are defined as any communication by a Credit Reporting Agency (CRA) of any information relating to a consumer’s “credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living” that is used or may be used in deciding the consumer’s suitability for employment or benefits, or eligibility for credit or insurance for personal, family or household purposes. It targets the uses of information, focusing on preventing harm from the subsequent use of credit reports rather than on limiting or allowing individuals to control collection. The core principles of the FCRA are notice, choice, and access.

64. Swire, supra note 22, at 1271.
66. For example, the California Security Breach Information Act, SB 1386, now requires notification of consumers in the event of certain security systems breaches; Vermont’s Department of Banking, Insurance, Securities, and Health Care Administration adopted opt-in provisions for information sharing, and Alaska (ALASKA STAT. § 06.05.175), Connecticut (CONN. GEN. STAT. ANN. § 36a-42), Illinois (205 ILL. COMP. STAT. ANN. 5/48.1) and Maryland (MD. CODE ANN. § 1-301) require some form of opt-in consent before financial information can be shared.
67. Financial Privacy and Consumer Protection: Second Session on the Growing Concerns Over the Way Consumers’ Personal and Financial Information is Being Shared or Sold by Their Financial Institutions: Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs, 107th Cong. (September 19, 2002).
69. Testimony of Fred Cate, supra note 67, at 7.
The FCRA divides financial information into two categories: (1) experience information and (2) eligibility, or application, information. While the FCRA does not restrict institutions from transferring identification, transaction, and experience information to affiliates or third parties, such information is covered as “nonpublic personal information” under the GLBA.

Before eligibility information can be shared with affiliates, the FCRA requires that financial institutions provide customers with notice and a reasonable opportunity to opt out. If the information is disclosed to a nonaffiliated third party, the financial institution becomes subject to significantly increased regulation as a CRA. Financial institutions must include the FCRA affiliate sharing opt-out notice along with its GLBA privacy notice. However, there are exceptions to the FCRA’s notice and opt-out provisions for insurance disclosures or disclosures permitted by government regulations.

Affiliates are prohibited from re-disclosing information received pursuant to an exception. The FCRA requires opt-in consent for very sensitive data sharing, including the transfer of personal medical information.

The Fair and Accurate Credit Transactions Act’s (FACTA) amendments to the FCRA provide that an entity that receives eligibility or experience information from an affiliate may not use that information to make marketing solicitations without providing clear and conspicuous notice to the consumer that information received from affiliates may be used for marketing purposes. The consumer must also have an opportunity and a simple method available to opt out of the sharing. A consumer may prohibit use of all information shared by affiliates for marketing purposes (including both eligibility and experience information generally covered by GLBA), subject to certain exemptions, such as when the affiliate receiving the information has a preexisting business relationship with the consumer. The consumer’s election to opt out is effective for five years but may be revoked, and states are preempted from regulating marketing covered by this provision. The FACTA legislation does not limit the ability of affiliates to share information, nor does it limit their ability to establish and maintain a database of information shared by affiliates; rather, it only requires notice of sharing before the information is used to send marketing solicitations.

The FCRA provides consumers with access to almost all the information

70. Banking Agencies’ Privacy Rule, supra note 46.
73. Other exceptions include: when the information is used to perform services on behalf of an affiliate, unless the affiliate would not be permitted to send the solicitation itself because of a consumer opt out; if the information is used to respond to contact initiated by the consumer or in response to solicitations authorized or requested by the consumer; and to comply with state insurance laws regarding unfair discrimination. L. Richard Fischer & Marcia Z. Sullivan, Privacy and the Fair and Accurate Transactions Act of 2003, A.L.I.-A.B.A. COURSE OF STUDY MATERIALS, Financial Services Institute 2004 (2004); CCH, supra note 59, at ¶ 10-062.
74. Ireland and Howell, supra note 16, at 688.
about them contained in CRA files and provides a mechanism by which they can have inaccurate or incomplete information removed or corrected. The Consumer Credit Reporting Reform Act of 1996 required credit reporting agencies to inform consumers of their legal rights under the FCRA and to delete any disputed data that they could not verify within 30 days, as well as comply with certain procedural requirements for correcting data and notifying recipients of disputed or inaccurate data. Report users must notify consumers of adverse actions taken based on the report and inform them that they may obtain a free copy of the report and dispute its accuracy with the CRA. In 2003, the FACTA further increased customers' rights of access, giving consumers a right to obtain a free annual credit report from nationwide CRAs and to obtain credit scores.

Although the FCRA has been described as largely self-enforcing, it is technically enforced by the FTC, which treats infringements of the FCRA as unfair or deceptive acts or practices in violation of the Federal Trade Commission Act (FTCA). Remedies for such practices include cease and desist orders, injunctions, and civil penalties. CRAs generally are required to follow "reasonable procedures" to ensure that their actions comply with the Act. Consumer suits for defamation, invasion of privacy and negligence in reporting information are generally prohibited unless false information was provided maliciously with the intent to injure the consumer. While prior to the GLBA, the FCRA was solely complaint-driven, the GLBA now allows for agency enforcement of the FCRA via the examination process.

Generally, the FCRA does not preempt state law unless the law is inconsistent with the FCRA. However, states may not alter certain FCRA provisions, even to provide more stringent regulation. For example, unalterable, or "uniform," provisions include those that address information sharing by affiliates, certain obligations of consumer report users, the rules placing limits on the age of information included in a report, and the responsibilities of persons who furnish information to CRAs. The FACTA permanently reauthorized the FCRA's national uniformity provisions, which were expected to sunset at the end of 2003. After the FACTA, the FCRA's consumer right to opt out of marketing solicitations by affiliates, as well as its requirement that creditors provide risk-based pricing notices and credit score disclosures also may not be altered by the states. Many of the important benefits to individuals and the economy from the current US reporting system, including greater access to

75. CATE ET AL., supra note 72, at 6.
76. Id. at 5.
77. See 16 CFR pt. 601.
81. In Bank of America v. City of Daly City, 279 F. Supp. 2d 1118 (N.D. Cal. 2003), a California District Court held that the affiliate sharing preemption provision of the federal FCRA preempts local privacy ordinances to the extent they purport to address affiliate sharing.
82. CCH, supra note 59, ¶ 10-075.
credit, more efficient markets, more accurate decision making, and consumer mobility and choice, have been said to result from the FCRA's national character.\textsuperscript{83}

The FACTA may limit consumers' abilities to enforce their rights under the FCRA. For example, it expands limits on liability for violations of the FCRA and restrains States from bringing actions for damages on behalf of their residents.\textsuperscript{84} Not all of the FACTA amendments have yet reached their effective dates.

\textbf{D. State Law, Self Regulation, and the Internet}

In addition to federal laws, States have also enacted financial privacy laws. Prior to the GLBA, several court decisions established a limited common law duty of confidentiality. For example, state courts have found it implicit in a bank's contract with its customers that the bank could not disclose information to third parties concerning the customer's account.\textsuperscript{85}

Furthermore, in response to consumer demand for privacy, many financial services providers have established privacy-related products and services, as well as options for individuals to control the use of their information, beyond what is required by law. In 2002, Professor Fred Cate stated: "Banks use privacy protection to compete for consumer business and have developed best practices for a variety of privacy protections. Citigroup has released telemarketing best practices developed with State attorneys general."\textsuperscript{86} Industry groups, such as the American Bankers Association (ABA), the Bankers Roundtable, and Consumer Bankers Association of America, announced joint industry privacy principles in 1997.\textsuperscript{87}

Independent third-party enforcement mechanisms promote compliance with self-regulatory codes. Online groups, such as BBB On-Line and TRUSTe, as well as the FTC and other federal agencies, have broad powers under the FTCA to enforce against "unfair and deceptive acts or practices," either by seeking injunctive relief or providing redress for injured consumers. All of the states

\textsuperscript{83} CATE ET AL., supra note 72, at 23.
\textsuperscript{86} Testimony of Fred Cate, supra note 67.
\textsuperscript{87} The ABA's eight privacy principles include using, collecting and retaining customer information only if the customer will benefit; establishing and maintaining customer financial information that is as accurate, current and complete as possible; protecting information via established security procedures; restricting disclosure of account information to situations where (a) the information is provided to help complete a customer initiated transaction; (b) the customer requests it; (c) the disclosure is required by/or allowed by law (i.e., investigation of fraudulent activity); or (d) the customer has been informed about the possibility of such disclosure and has the opportunity to "opt out"; and making an institution's privacy principles or policies known to the customer. See American Banking Association, "Financial Privacy in America: A Review of Consumer Financial Issues" (June 1998), http://www.aba.com/About+ABA/ABA_privprinpublic.htm (last visited Apr. 27, 2005).
have enacted laws similar to the FTCA to prevent unfair or deceptive acts.

Furthermore, better privacy policies, although reducing the ease of information sharing, may even enhance efficiency. As Swire explains, because of increased consumer trust, banks with better privacy policies may experience higher rates of customer participation in other services, such as online banking, and banks that provide clear and explicit notice of the customer of the right to opt out may not experience a higher rate of opt-out requests.88 Stronger privacy practices have even been correlated with a lower likelihood of customers exercising their right to block data sharing.89 Electronic and online banking pose a range of new problems concerning the security of consumer information provided via the Internet. The FTC, which regulates individual and commercial online privacy, found in 2000 in its Report on Online Privacy that industry self regulation was inadequate to counter the significant privacy concerns raised by the Internet, and it called for federal privacy legislation to address this issue.90 However, to date, most of the online privacy statutes are directed toward children or toward specific abuses91 and the FTC has not imposed a general privacy policy disclosure requirement on website operators, focusing instead on whether a company's practices are consistent with its privacy policy. However, states may be more aggressive in passing online privacy legislation.92

E. Insurance

The GLBA calls on state insurance authorities to enforce its provisions by adopting information disclosure and safeguards regulations. To facilitate implementation, the National Association of Insurance Commissioners issued a Model Regulation in 2000, the “Privacy of Consumer Financial and Health Information Regulation,” that substantially conforms to the regulations adopted by the federal agencies. The 2000 regulation follows the Insurance Information and Privacy Protection Model Act adopted by the NAIC in 1982, which established an affirmative consent (“opt-in”) standard for disclosure of consumers’ personal information.93 Currently, 35 states have adopted the 2000

88. See Swire, supra note 19.
89. For the top five banks, where customers reported a much higher awareness of the privacy policy, only 8% said that they had ever requested that their bank stop using or sharing their personal information. By contrast, for the bottom five banks, where relatively few customers are even aware of the privacy policies, 14% of customers had prevented data sharing. Id.
Model Regulation, and the remaining states have amended the regulations they had in place pursuant to the 1982 Model Act. Some states have opt-in requirements, or are otherwise more protective of consumer privacy than required by the GLBA. The notice required by the 1982 Act is more detailed than that provided by the GLBA, but, like the GLBA, it contains no restriction on affiliate sharing. The NAIC Act contains an “access” provision, and it provides for investigation of violations of security and enforcement provisions, providing individual remedies in some cases.

III. DATA PROTECTION IN THE EUROPEAN UNION

A. Historical Overview of Data Protection

The European right to privacy was initially articulated in the United Nations’ (UN) Universal Declaration of Human Rights (1948) and the landmark Council of Europe Convention on Human Rights and Fundamental Freedoms (1949). This approach to information privacy in Europe is derived in part from invasions of privacy at the root of certain World War II abuses and in part from a tradition of prospective lawmaking that seeks to guard against future harms, particularly where social issues are concerned. In 1968, the Council of Europe recognized the potential of the computer to threaten individual privacy, and in 1970, the German State of Hesse adopted the world’s first national data protection law. Sweden’s Data Bank Statute followed swiftly on its heels in 1973, and by the end of the 1970s, seven members of the Council of Europe had adopted national data protection laws.

94. See GAO Report, supra note 26, at 3.
95. See, e.g., the New Mexico Privacy Rule, 13 NMAC 1.2.1 TO 28, available at http://www.nmprc.state.nm.us/insurance/pdf/insbul23003.pdf.
96. Sammin, supra note 93, at 668-69.
97. Id. at 669.
100. Wellbery, supra note 17.
102. BAINBRIDGE, supra note 99, at 14.
103. The Swedish statute protects data in automatic processing systems containing personal information and creates a Data Inspection Board. Cole, supra note 101, at 902.
However, compliance with national laws proved insufficient to protect consumer information as nation-states became increasingly part of a global financial network in which companies located their processing operations outside the country of origin. National data protection legislation produced conflicting standards, and concerns about "data havens" and outsourcing emerged.

The OECD initiated the first attempt to implement privacy standards at an international level when, in September 1980, it adopted a recommendation urging member countries to take into account a set of eight guideline principles on the protection of privacy. The problem with the OECD guidelines was that they were merely prefatory, with no mechanism for enforcement. A year later, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which contains provisions similar to the Guidelines and emphasizes data protection as a key to personal privacy. Its provisions are still considered the blueprint for a minimum standard of protection in national law. However, the binding force of a Council Directive was necessary. As data protection guarantees became increasingly important to trade, the Commission sought to create a regulatory framework to harmonize widely divergent national legislation, ensure proper functioning of the Single Market, and prevent states from enacting protectionist policies. The formal basis for the Data Protection Directive is the strong link between data processing and economic activity under Article 100a (now Article 95) of the EC Treaty (intended to ensure "the establishment and functioning of the Internal Market"). In 1995, the European Council adopted Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive" or "Data Protection Directive"). The Directive required Member States to enact implementing legislation by 1998.

104. BAINBRIDGE, supra note 99, at 15.
105. Id. at 15-16. The OECD principles include: (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) openness; (f) security safeguards; (g) individual participation; and (h) accountability.
108. In 1999, the Commission took France, Germany, Ireland, Luxembourg and the Netherlands to the European Court of Justice for failure to notify all the necessary measures to implement Directive 95/46. Currently, all of the Member States have notified compliance with the Directive, and the cases have been settled. In line with the Copenhagen criteria, the countries that joined the EU on May 1, 2004 transposed Directive 95/46/EC by the time of accession. However, in its First Report on the Implementation of the Directive, the Commission stated that further efforts would be needed to bring this legislation fully into line with all provisions of the Directive, particularly by establishing independent data protection supervisory authorities. While the range of existing supervisory authorities differs, "all the supervisory authorities lack the necessary resources and some also the necessary powers to ensure effective implementation of data protection legislation." European Commission First report on the Implementation of the Data Protection
Although each country locates the right to privacy in a range of traditions and legal and constitutional rights, privacy is widely considered by most European legal bodies as a “fundamental right.” The Directive states that “the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy.”\textsuperscript{109} In 2000, the fundamental importance of data protection was reinforced in the European Charter of Fundamental Rights of the European Union of 2000.\textsuperscript{110} Furthermore, the recently finalized Treaty Establishing a Constitution for Europe, signed on October 29, 2004, recognizes that “everyone has the right to the protection of personal data concerning him or her.”\textsuperscript{111} Privacy legislation is therefore not sector-dependent but applies absolutely to all personal data processing, whether by the government or by private entities. There are no privacy laws that apply uniquely to the financial services sector.\textsuperscript{112}

**B. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data**

The Data Protection Directive serves the dual purpose of ensuring the free movement of personal data in the Internal Market and guaranteeing a uniformly high level of privacy protection for data subjects.\textsuperscript{113} Directives in the EU are not directly binding but rather provide broad legal norms that must be implemented by Member States in national legislation. If the Commission considers that a Member State has failed to implement a directive appropriately in national law, it may challenge the State in the European Court of Justice (“ECJ”).\textsuperscript{114}

The Data Protection Directive outlines eight basic personal data protection principles, which are derived from the OECD Guidelines and Article 8 of Convention 108. First, the “purpose limitation” principle stipulates that data should be processed for a specific purpose and subsequently used or communicated only in ways consistent with that purpose. Second, the “data

---

\textsuperscript{109} Data Protection Directive, Preamble, at 10.

\textsuperscript{110} 2000/C 364/01, the European Council of Nice on the 6\textsuperscript{th} of December of 2000. Chapter II on “ Freedoms” provides that “everyone has the right to the protection of personal data concerning him or her.” \textit{Id.} art. 8(1). Furthermore, personal data must be “processed fairly for specified purposes and on the basis of the consent of the person concerned” or on another legitimate basis expressly granted by law. \textit{Id.} art. 8(2). The Charter grants to every person the right of access to and rectification of data which has been collected concerning him or her. \textit{Id.} art. 8(2). The Charter also specifies that compliance with data protection principles must be subject to control by an independent authority. \textit{Id.} art. 8(3).


\textsuperscript{112} An exception is the professional secrecy provision in the Banking Directive.

\textsuperscript{113} See Data Protection Directive art. 1.

\textsuperscript{114} See Treaty Establishing the European Community, art. 226, Nov. 10, 1997, 1997 O.J. (C 340) 3. Specific aspects of a directive may be found by the ECJ to be “directly applicable” to private citizens. For examples of cases brought against Member States for failure to implement the Data Protection Directive (95/46/EC), see \textit{supra} note 108.
quality and proportionality” principle requires data to be accurate and, where necessary, kept up to date. Third, the “transparency” principle dictates that individuals should be informed of the purpose of the processing and the identity of the data controller. Fourth, the rights of “access, rectification and opposition” include the data subject’s rights to obtain copies of all data relating to him or her that are processed, to rectify inaccurate data, and to object to processing in certain situations. Fifth, the “security” principle ensures that the data controller takes technical and organizational security measures appropriate to the risks of the processing; it also requires that processors acting under the authority of the controller process data only upon the controller’s instructions. Sixth, the Directive’s “restriction on onward transfers” to third countries that do not afford “adequate” levels of protection guarantees that the level of protection in the Community will not be undermined by controllers sending data abroad for processing. Seventh, additional protections must be applied to sensitive data, data used for marketing purposes, or data subject to automated processing. Finally, the Directive emphasizes enforcement and remedies for data subjects.

The Directive applies to “personal data,” or “any information relating to an identified or identifiable natural person,” if that data is processed “wholly or partly by automatic means” or as “part of a filing system.” The Directive does not cover “purely personal or household” use or processing in the course of an activity which falls outside the scope of Community law, such as public security, defense, and State security. Member States differ as to whether corporate data should be treated as personal data, and some States have further limited the scope of personal data. The broad notion of “processing” refers to any operation or set of operations performed upon personal data. The laws enacted pursuant to the Directive apply to “data controllers” or “processors” located in a Member State, in a territory subject to the Member State’s laws, or elsewhere if the controller or processor makes use of equipment located on the territory of the Member State for purposes other than simple transmission.

Member States may enact measures in contravention of the Directive if necessary in the interest of national security, defense, public security; the prevention, investigation, detection, and prosecution of criminal offences; an important economic or financial interest of a Member State or of the EU; a monitoring, inspection, or regulatory function connected with the exercise of

116. Id. art. 3(1).
117. Id. art. 3(2).
119. In Britain, for example, “personal data” was found not to refer merely to a person’s name mentioned in a document. See Durant v Financial Services Authority, [2003] EWCA (Civ) 1746, [1]-[81] (Eng.), available at http://www.hmcourts-service.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm.
120. Data Protection Directive art. 2(b).
121. Id. art. 4(1).
official authority; or the protection of the data subject or of the rights and freedoms of others.122

1. Purpose Limitation, Data Quality and Proportionality

Under the Directive, personal data must be processed “fairly and lawfully.”123 Article 6 specifies that data may be collected only “for specified, explicit and legitimate purposes,” and it must not be “further processed in a way incompatible with those purposes,” with a limited exception for data processed for historical, statistical or scientific reasons. Furthermore, the data must be “adequate, relevant and not excessive,” given the purposes for which it is acquired. It must be accurate and, where necessary, “kept up to date.” “Every reasonable step” must be taken to ensure that inaccurate or incomplete information is either erased or rectified. Finally, data must be kept in a form which permits identification of the data subject for “no longer than necessary” for the purposes for which it was collected or processed.124

Currently there is some tension between the different Member States’ implementing legislation as to how long data may be kept before it must be deleted.125 Furthermore, within some Member States, there are conflicts between the length of time that data must be retained under applicable financial law and the limits on the length of time it may be retained under the local Data Protection laws.126 With respect to the “incompatible use” criterion, Member State laws vary in the range of uses they will permit. Some States provide more flexibility if the controller is a financial institution that already has a special duty of confidentiality.127

Data processing may occur only if the “data subject has unambiguously given his consent”128 unless processing is necessary for one of several reasons. For example, processing may be necessary for the performance of a contract to which the data subject is a party; for compliance with a legal obligation to which the controller is subject; in order to protect the data subject’s vital interests; for the performance of a task carried out in the public interest or in the exercise of official authority; or in order to serve the legitimate interests of the controller or a third party to whom the data is disclosed.129 However, these exemptions do not enable processing where the interests served are overridden by the fundamental rights and freedoms of the data subject. The “unambiguous consent” standard has been interpreted as an opt-out requirement for all but the

122. Id. art. 13(1).
123. Id. art. 6(1).
124. Id.
125. Citigroup, supra note 118, at 3.
126. Id.
128. Data Protection Directive art. 7(a).
129. Id. arts. 7(b)-(f).
most sensitive data sharing.

2. Transparency

The data controller or his representative must notify the appropriate national supervisory authority before carrying out any automatic data processing operation.\(^{130}\) Member States may exempt operations or transactions from the notification requirement, or simplify the notification process under certain circumstances such as where the controller appoints a "personal data protection official" responsible for ensuring the internal application of the national data protection provisions.\(^{131}\) If notification is required, it must include the name and address of the controller and his representative; the purpose or purposes of the processing; a description of the categories of data subjects and of the categories of data relating to them; the categories of recipients to whom the data may be disclosed; the proposed transfers of data to third countries; and a general description of the measures taken to ensure security of processing that will allow the supervisory authority to make a preliminary assessment of their appropriateness.\(^{132}\)

In addition, Member States must determine which processing operations are likely to present specific risks to the rights of data subjects and examine these operations prior to their commencement.\(^{133}\) Member States must ensure that processing operations are publicized and that a register of notified processing operations is made available for public inspection.\(^{134}\) For processing not subject to notification, the controller or "another body appointed by the Member State" must make the basic Article 19 notification information available to any person on request.\(^{135}\) It is widely agreed that notification currently serves little real purpose and takes up an excessive amount of resources.\(^{136}\)

3. Rights of Access, Rectification and Opposition

The Directive specifies that certain information must be provided directly to the data subject. Specifically, the data subject must be informed of the identity of the controller and any representatives, the intended purposes of the processing, and any further relevant information (such as rights of access and rectification, recipients of the data, etc.) that is necessary to "guarantee fair processing."\(^{137}\) Member States' laws vary considerably with regard to the kinds

\(^{130}\) Id. art. 18(1).
\(^{131}\) Id. art. 18(2).
\(^{132}\) Id. art. 19(1).
\(^{133}\) Id. art. 20(1).
\(^{134}\) Id. arts. 21(1)-(2).
\(^{135}\) Id. art. 21(3).
\(^{136}\) Korff, supra note 127, at 165.
\(^{137}\) Data Protection Directive art. 10. If the data was not obtained from the data subject, the controller must disclose the same information as above to the subject either when the personal data is
of information that must be provided, the form in which it must be provided, the
time at which it must be provided, and the types of additional information that
may be required to ensure “fairness.”138

Data subjects’ rights are central to data protection in the EU because they
are the primary means of asserting the “informational right to self-
determination.”139 In addition to the rights to obtain, correct, or erase
processing information and to object to direct marketing use of personal data,
the Directive provides data subjects with a general right to object, as well as a
special right not to be subject to certain “fully automated
decisions.”140

A data subject’s “right of access” allows the subject to find out from the
controller in “an intelligible form” whether data relating to him or her are being
processed, the purpose of processing, the types of data involved, the identities of
the data recipients, and any information as to their source, as well as the logic
involved in any automatic processing.141 “As appropriate,” the controller must
grant the subject rectification, erasure, or blocking of data whose processing
does not comply with the Directive and must provide notification to third parties
to whom the data has been disclosed of any rectification, erasure, or blocking
carried out, unless such notification is impossible or “involves a
disproportionate effort.”142

The data subject may object to the processing of his data at any time based
on “compelling legitimate” grounds relating to his particular situation, at least
where the processing is performed in order to serve the “public interest” or the
legitimate interest of the controller.143 Where the objection is “justified,” the
controller must stop processing the data. However, there are significant
differences in the implementation of the right to object; some Member States
extend this right to all, or most, processing, while others do not provide for this
right at all.144

A data subject’s objection to processing is presumptively justified if the
data is to be used for direct marketing purposes.145 Member States have two
alternatives for guaranteeing data subjects’ right to object to the disclosure or
use of their data for direct marketing purposes.146 First, the data subject may
object to the processing of personal data that the controller anticipates will be

initially recorded or no later than when the data are first disclosed to a third party. However,
disclosure to data subjects about whom data has been acquired indirectly is not required where it is
impossible or would “involve a disproportionate effort.” See Data Protection Directive, arts.11(1),
11(2).

139. Id. at 105.
140. Id.
142. Id. art. 12(c).
143. Id. art. 14(a).
144. Korff, supra note 127, at 105.
146. Korff, supra note 127, at 113.
processed for direct marketing purposes. If a Member State chooses to give the data subject this right, it must take "necessary measures" to ensure that the data subject is aware of how to exercise it. A "necessary measure" could be providing appropriate publicity about the existence of such a right. Second, the subject must be "informed before personal data are disclosed for the first time to a third party for direct marketing and expressly offered the right to object free of charge to such disclosures or uses." Under this second option, data subjects must be expressly offered the right to object to direct marketing "uses or disclosures" of their data. While there are differences in Member State implementation of this provision, most States maintain suppression lists to which individuals can subscribe in order to avoid having their data processed for direct marketing.

Finally, every person has the right not to be subject to a decision which "significantly affects him" if the decision is based solely on automated processing of data intended to evaluate certain "personal aspects" relating to him. However, a person may be subject to an automated decision if it is made in the course of performing a contract, if the data subject requested to enter into the contract, or if there are "suitable safeguards" of the subject's legitimate interests. Generally, Member States differ in their national provisions for objections to automated decisions as well as for direct marketing use.

4. Security

The Directive requires data controllers to "implement appropriate technical and organizational measures" in order to protect personal data against "accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access . . . and all other unlawful forms of processing." The measures must guarantee a level of security "appropriate to the risks" of the processing, taking into account the cost of implementation and the state of the art. Controllers are responsible for ensuring that their processors provide sufficient guarantees of adequate technical and organizational measures for the processing.

5. Restrictions on Transfers Outside of the EU

Personal data may only be transferred to a party in a non-Member State for processing if that state ensures "an adequate level of protection."
“Adequacy" is to be assessed in light of all the circumstances surrounding a data transfer operation, including the nature of the data; the purpose and duration of the proposed processing operations; the countries of origin and destination; the laws (both general and sectoral) in force in the non-Member State; and its "professional rules and security measures." When the Commission finds that a third country does not provide an adequate level of protection, Member States must "take the measures necessary" to prevent personal data transfers to that country.  

Member States may provide exceptions to transfer restrictions if certain conditions are met, such as when the data subject has given "unambiguous consent" to the proposed transfer. The transfer is also lawful if it is necessary for the performance of a contract between the data subject and the controller or a contract concluded in the interest of the data subject between the controller and a third party; if it is necessary or legally required on important public interest grounds; or if it is necessary to exercise a legal claim or "protect the vital interests of the data subject."

Furthermore, a Member State may authorize a set of transfers to a third country where the controller adduces adequate safeguards of privacy, such as those provided by appropriate contractual clauses. If the Commission determines that certain standard contractual clauses offer sufficient safeguards, Member States are bound by its decision. While the laws of almost all Member States prohibit transfers to third countries without adequate data protection laws, some countries have also implemented laws focused on the “adequacy" of the protection offered by the recipient in a third country. The Directive itself calls for the drawing up of quasi-self-regulatory “codes of conduct" that are tailored to take account of specific features of various economic sectors and are largely self-enforced.

Article 29 establishes and grants independent advisory status to a “Working Party on the Protection of Individuals with regard to the Processing of Personal Data.” The Working Party (WP) is composed of a representative of each supervisory authority of each Member State, the authorities for the Community institutions and bodies, and the Commission. It advises the Commission on data protection issues and provides opinions on the levels of protection in the Community and in third countries.

155. Id. art. 25(2).
156. Id. art. 25(4).
157. Id. art. 26(1)(a).
158. Id. art. 26(1)(e).
159. Id. art. 26(2).
160. Id. art. 26(4).
162. Data Protection Directive art. 27(1).
163. Id. art. 30.
6. Sensitive Data

The Directive carves out a special category for sensitive data, defined as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership," and data concerning "health or sex life."164 Such data may be processed only if the data subject gives "explicit consent" to processing. In the absence of explicit consent, processing may occur only if it is necessary to carry out the obligations and rights of the controller as authorized by national law; to protect the vital interests of the data subject; if the data have been made public by the data subject; if the processing is carried out in the course of legitimate activities by a non-profit-seeking body; or to establish, exercise, or defend legal claims.165 Member States may create exceptions to these added protections for reasons of substantial public interest or law enforcement.

Most of the personal data collected by banks and other financial service providers relating to clients is not considered "sensitive" under Article 8(1) of the Directive.166 However, some Member States add or assign special treatment to further categories of data they consider sensitive, such as debts, financial standing, and the payment of welfare benefits.167

7. Enforcement and Remedies

In addition to administrative remedies, every person must be guaranteed a judicial remedy for any breach of the rights guaranteed by the Member State’s national data protection legislation.168 In most countries, ordinary civil and administrative liability rules apply.169 All states allow subjects to seek redress through the courts, although damages vary from state to state.170 All the laws also contain extensive penal provisions, characterizing breaches of data protection laws as criminal offences, punishable by fines or imprisonment.171 A party injured by unlawful processing is presumptively entitled to receive compensation from the controller for the damage suffered.172

The Directive requires that each Member State establish independent supervisory authorities, usually called Data Protection Authorities (DPAs), which are responsible for monitoring the application of data protection legislation.173 These supervisory authorities hear claims by individuals or associations and each authority has powers of investigation and intervention,

164. Id. art. 8(1).
165. Id. art. 8(2).
166. BAINBRIDGE, supra note 99, at 157.
170. Id. at 179.
171. Id. at 180.
173. Id. art. 28(1).
including the power to "engage in legal proceedings" when national data protection provisions have been violated.

Member States must also lay down sanctions for infringement of national data protection laws. However, the DPAs in all the Member States rarely apply formal sanctions; most matters of contention, including manifest breaches of the law, are dealt with through discussion and negotiation. Criminal prosecutions are extremely rare. In practice, the most important function of sanctions may be to greatly improve the DPAs' negotiating position.

The EU has recently enacted several directives aimed specifically at online and telecommunications privacy. These directives generally uphold and reinforce the data protection principles of Directive 95/46/EC.

C. The European Court of Justice's Interpretation of the Directive

The ECJ, established in 1952 by the Treaty of Paris, ensures that "Community Law" is interpreted and applied in the same way in each Member State. An ECJ decision is binding on national courts of the EU Member States. The ECJ's decisions in the Rechnungshofer and Lindqvist cases establish that Directive 95/46/EC can be applied broadly. In Rechnungshof, the Court interpreted the scope, applicability, and legal basis of the Directive for the first time. It considered the validity under the Directive of a German law requiring certain employers to disclose to a government agency the salaries of specific employees if they exceeded a certain amount. The ECJ held that the Data Protection Directive applied because the national law was adopted to enhance the functioning of the internal market and was thus considered a "Community Law." The applicability of the Directive did not depend on whether the processing had an actual connection with freedom of movement between Member States. The Court went on to uphold the general applicability of the Directive's provisions in Articles 6(1)(c) and 7(c) and (e). These provisions...
require that data must be "adequate, relevant, and not excessive" in relation to the purposes of collection, and that it must be collected pursuant to legal obligations of the controller in order to enable performance of a task carried out in the public interest. The ECJ found that these provisions state "unconditional obligations" that may be directly applicable in a national court.¹⁸¹

The ECJ remanded the case to the national court to determine whether the law could be interpreted in a manner consistent with the Directive.¹⁸² It found that the law could meet the conditions for exemption under Article 13 of the Directive, which allows States to enact laws in order to safeguard certain public interest goals, including "an important economic or financial interest of a Member State."¹⁸³ Finally, the Court emphasized that the Directive's provisions governing the right to privacy in the processing of data have the status of fundamental rights and general principles of Community Law.¹⁸⁴

IV.
COMPARISON OF US AND EU FINANCIAL PRIVACY PROTECTION

Comparative legal scholars have remarked that "privacy law is part of a national legal system and must be fitted into this system with proper respect to its legal environment and national institutions."¹⁸⁵ The legal instruments used to address privacy concerns depend on how privacy is defined and what values it is perceived to serve.¹⁸⁶ Despite divergent approaches to privacy, similar levels of protection may be achieved overall. The more pragmatic US approach to creating and applying data protection laws has thus far precluded a determination by the EU as to whether the US financial sector meets the basic European data protection requirements. A meaningful analysis of adequate protection from a functional perspective must comprise "two basic elements: the content of the rules applicable, and the means for ensuring their effective application."¹⁸⁷

This Part will first consider "the content of the rules applicable," including a discussion of the most significant differences in actual privacy standards in the financial services industry in the US and the EU. These include: (a) the scope of information subject to regulation, including the fact that the US does not have a single broad data protection law; (b) data subject access to personal information held by a data controller; (c) standards of consumer control over the secondary uses of personal information, particularly with respect to information sharing

¹⁸¹. Id. ¶¶ 100, 101.
¹⁸². Id. ¶ 93.
¹⁸³. Data Protection Directive art. 13(1)(e); Case C-465/00, supra note 178, ¶ 67.
¹⁸⁴. Id. ¶¶ 68-69.
¹⁸⁶. CATE, supra note 4, at 129-30.
with affiliates, joint partners or in a marketing context; and (d) special treatment of sensitive information. In considering the content of the data protection laws, this paper aims to analyze the systems from a “functional similarity” perspective, which “looks for the aggregate, substantive standards applied to the treatment of personal information in the United States.”  

The pragmatic and sectoral approach to data protection in the United States creates a system in which the overall standards emerge from a complex interplay of state and federal regulations, as well as industry practices. In contrast, the EU’s global approach uses broad strokes to delineate overall standards, yet these standards are enforced in such a way that the actual, functional protections provided may be more pragmatic and limited than they appear from the language of the Directive itself.

Next, this Part will consider enforcement of these legal standards, or the “means for ensuring their effective application,” including the existence of a private right of action and the effectiveness of self regulation in establishing de facto privacy standards. US law is premised on the idea that self regulation, backed by enforceable legislation where there are risks of serious harm, can be effective. In the EU, self-regulatory measures are increasingly accepted as valid mechanisms for enforcement only to the extent that they can be shown to provide a good level of compliance, support for the data subject in exercising her enforcement rights, and appropriate individual redress.  

The self-regulatory measures of the US, analyzed under this enforcement rubric, provide substantial safeguards that the EU should recognize.

A. Scope of Protection

The Data Protection Directive covers certain types of personal data and certain forms of processing that receive little formal legal protection in the US financial regulatory system, including non-financial data, certain types of processing operations, and certain data processed both within and outside the regulator’s territory. However, when considered from a functional perspective and in the context of the financial sector, these discrepancies may not be as serious as they appear.

First, one of the EU’s major concerns is the absence of a “horizontal law” in the United States, similar to the Directive, which would cover any sort of processing of personal data. In the United States, while privacy regulation of the financial sector is substantial, other industries are largely unregulated for privacy. Europeans may argue that, although processing of EU citizens’ personal data may be adequately protected within US financial institutions,
weak regulations in other sectors put their personal information at risk. In particular, the EU may be concerned that there are inadequate safeguards for transfers to non-financial entities and other countries that do not provide adequate protection.

With respect to transfers to non-financial entities unregulated under the GLBA or the FCRA, there are some safeguards in place, and the absence of omnibus legislation has not prevented European determinations that certain entities in the US (such as those that have agreed to abide by the US-EU Safe Harbor or the approved Model Contracts) provide “adequate protection” for personal data. It is true that US financial institutions can now share information freely with affiliates that are not traditionally conceived of as “financial,” and non-financial third parties can receive nonpublic personal information pursuant to the notice and opt-out provisions. However, GLBA restrictions on further use also apply to non-financial recipients of data, and in theory, customers may opt out of third-party sharing altogether. More importantly, the EU accepted notice and choice in the Safe Harbor as sufficient safeguards for onward transfers. In the Model Contracts, the “purpose limitation” is adequate, and the levels of protection in other sectors are not considered.

Even for financial data, the Directive’s definition of “personal data” covers more information than the GLBA’s “nonpublic personal information.” “Personal data” under the Directive is defined as “any information relating to an identified or identifiable natural person,” whereas “nonpublic personal information” under the GLBA includes any personal financial information that is obtained by the financial institution. The FCRA only covers information used in making credit decisions. As a result, the Directive applies to certain public information about individuals, professional data, and encrypted data if the controller has both the data and the “key” to interpret it. However, these types of information, not covered in the US but covered by the Directive, are arguably not likely to give rise to abuses that harm individual consumers. Encrypted information is less easily misappropriated, public information has already been released to those who may misappropriate it, and corporate information, which is not even consistently covered in the EU States’ national laws, poses no obvious threat to the individual’s right to privacy.

The Directive also covers data “processing” as “any operation performed upon personal data.” This definition renders the data protection laws applicable

---

191. See infra note 352.
195. In the UK, for example, the Information Commissioner’s Office finds that professional data does not normally require application of the full panoply of data protections. Andrew Charlesworth, Symposium: Enforcing Privacy Rights: Thinking About Optimal Enforcement: Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?, 54 HASTINGS L.J. 931, 942 (2003).
to almost all types of processing operations, including profiling and other identity analysis. However, while the European Court of Justice interpreted “processing” broadly in *Lindqvist* to include posting material on a website, it seems impractical that the terms of the Directive would be enforced against every activity pertaining to data on open networks. Because such broad enforcement is implausible, the actual standard for applying the Directive is somewhat unclear. Nevertheless, the most significant discrepancy may be that, under the GLBA, consumers may not be able to prevent “profiling” of information that is not covered under the FCRA as eligibility information. However, for credit information, the FACTA requires disclosure of the score generated by the agency’s computer model as well as “all of the key factors that adversely affected the credit score of the consumer in the model used.” In addition, common law torts of “intrusion on seclusion,” “breach of confidentiality,” and “appropriation privacy," may offer effective weapons against profiling by financial institutions. As a result, the scope of processing that is actually covered in the United States may not differ significantly from that covered in the EU.

Significantly, the Directive covers broad geographic territory in order to prevent outsourcing or the creation of data havens that undermine data protection standards and hinder the free flow of information in the Internal Market. First, the Directive covers any controllers and processors that use equipment located in a Member State or its territories. While the Directive is technically limited to matters that fall within the scope of “Community Law,” the ECJ has interpreted the Directive’s application broadly. It has held that, as long as a Member State law is “intended to improve the conditions for the establishment and functioning of the Internal Market,” it falls within the scope of Article 100a of the Treaty establishing the European Community. This renders the Directive applicable to situations that otherwise may not have ties to the EU. Finally, the Data Protection Directive covers the personal data of EU citizens processed in a third country.

In contrast, US federal legislation applies only to certain information processing activities of US financial institutions subject to the jurisdiction of one of the eight federal regulatory agencies or, in the case of insurance, to state insurance agencies. The FTC has stated that there are no legal restrictions on financial services companies' sending customer data abroad for processing. However, in practice, while financial institutions may outsource data processing

197. FACTA § 212(b), amending FCRA § 609(f), 15 USC § 1681(g) (2006).
198. See Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 993-94 (2002) (providing a general description of these torts and their application to financial institutions, including in particular where there is a “reasonable expectation” of privacy in financial information).
199. Case C-465/00, *supra* note 178, ¶ 41.
operations for economic reasons, if they violate basic privacy expectations of US consumers, they may be subject to lawsuits under state laws, in addition to receiving substantial negative publicity. Furthermore, although financial institutions do not have to disclose whether they are sharing nonpublic personal information with service providers outside the United States pursuant to joint marketing agreements, they are legally responsible under the GLBA for ensuring that their joint service providers "maintain the confidentiality" of that information. In any event, more stringent legislation is currently pending with respect to transfers of personal data abroad; as of August 2004, there were almost 200 bills in Congress that would curb outsourcing. Representative Edward J. Markey (D-Mass) vowed "to close down these privacy loopholes." The FDIC released a report in June 2004, "Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risk," outlining five major risk areas, including lack of sufficient internal operational and transactional controls. However, thus far, there have been surprisingly few breaches of consumer privacy by data processors abroad. There are some indications that India, an outsourcing hub afraid of losing North American and European business if it violates privacy standards, may be voluntarily adopting very high standards of privacy, especially with respect to security and confidentiality.

Furthermore, Article 25's restrictions on transfers have been found to be inadequately enforced in many countries, and there is evidence that EU financial institutions are also outsourcing. While the EU may perceive the theoretical right to prevent transfers as a greater substantive right, in practice, it may not provide European citizens with more real protection than US citizens who have no benefits of "adequacy determinations." Some argue that institutions that decide to outsource for financial reasons will find ways to do so. For example, a strategic policy manager at the UK's Data Protection Registry stated: "Companies have found ways round the law. They often use a contractual relationship with the Indian subsidiary or subcontractor that binds them to acting as if the UK's law was in force. We have had few complaints

202. Heller, supra note 200. The world's 100 largest financial services companies expect to transfer about $356 billion of their operations and two million jobs offshore over the next five years, according to Deloitte Research, a division of Deloitte Consulting LLP. Jeremy Quittner, Offshoring Can Cut Costs, But It Raises Risk, AM. BANKER, July 6, 2004.
203. Quittner, supra note 206.
204. Chester, supra note 201.
205. Id. Chester states: "To reassure their North American customers, Indian outsourcers are installing state of the art surveillance and monitoring equipment that is so intrusive that it would scarcely be tolerated in a North American workplace. Indian staff works under security cameras and at terminals that lack printers, hard drives and e-mail—workers cannot copy any data. Rigid confidentiality pledges are the norm.... India's fear is that security and privacy concerns will become non-tariff barriers to trade in services and information technology."
from consumers, so we think that, by and large, this means it is being handled well." Other companies, such as HSBC, claim that they have permission from customers, based on a set of revised conditions sent to customers. An absence of complaints may support the argument that outsourcing centers are voluntarily policing information abuses.

In sum, the disparities between the scope of covered processing in the United States and the European Union are actually less significant than they may appear, and they are not relevant for a sectoral adequacy determination. The existence of a single horizontal law is not required, as indicated by the EU’s acceptance of the Safe Harbor and Model Contracts. The categories of personal data not covered in the United States are less likely to pose real harm to consumers, and the concerns with respect to profiling can be largely dealt with through the FCRA and state laws. Finally, the difference in territorial scope may in practice be less significant than it appears, and the United States is already willing to pass more stringent legislation to protect against outsourcing of personal data.

B. Data Subject Access to Personal Information

While the GLBA lacks a consumer access provision similar to the European Data Protection Directive’s provisions for data subject access, the FCRA contains broad access provisions comparable to those of the Directive. Furthermore, in practice, US consumers often have access to their personal financial information and individuals generally receive detailed records for checking accounts, credit card records, and securities brokerage accounts. They can contest the accuracy and completeness of those records as problems arise. Even privacy lobbyists admit that “consumers generally have access to review and dispute their account statements.” In addition, the Fair Credit Billing Act (FCBA) allows customers to contest certain billing aspects of their transaction histories. The scope of the right to rectify or erase inaccurate information is not any greater than that provided under the FCRA for credit reports, where errors can have the most significant impact.

First, under the GLBA, consumers have no explicit rights to review or dispute the development of detailed profiles on them created by financial institutions based on their transaction information. In contrast, under the FACTA, consumers have access to their credit scores. The US approach focuses on preventing the potential harm; under the FCRA, any adverse action taken

208. Id.
209. Swire, supra note 22, at 1269-70.
210. Id. at 1270.
against a consumer as a result of a profile must be disclosed to the consumer in addition to the consumer's personal information on which the profile was based. The consumer must be able to exercise her right to access such information, correct it, and have the correction passed on to any other institutions that received the erroneous information. In the EU, Member States themselves differ on the right to be informed of the "logic" used in certain decisions, although all States provide this right with respect to completely automated processing.\(^{212}\) The right to understand the internal logic of the controller's processing operations does not appear to be as crucial to preventing consumer harm as the right to rectify or erase inaccurate facts.

Second, other US laws have access provisions that apply to financial information held by financial institutions. For example, laws provide for customers to receive images of their returned checks or personal checks after processing.\(^{213}\) In addition, the Fair Credit Billing Act, applicable to "open end" credit accounts, such as credit cards and revolving charge accounts, provides settlement procedures for disputes about billing errors.\(^{214}\) Businesses that offer this type of credit must provide written notice describing the customer's right to dispute billing errors. If a customer legitimately objects to a charge and demands rectification, the institution must determine whether the bill contains an error, and if it does, the creditor must credit the account and remove all finance charges, late fees or other charges related to the error. The creditor must explain to the customer, in writing, the corrections that will be made to the account. Moreover, standard industry practice generally dictates that customers have access to personal financial files in the ordinary course of business; most banks send out account statements monthly and provide ongoing online or phone access to one's account.\(^{215}\) Thanks to the longstanding nature of these practices, consumers have come to expect and demand them.

State laws also provide certain access rights. For example, customers may pursue state law contract and tort claims if an institution breaches a stated policy of granting customers access to files containing their personal information.

Currently, two bills are pending in Congress that would require customer notification of any security breach that occurs at the financial institution relating to that customer's data.\(^{216}\) In addition, federal financial regulators have

\(^{212}\) Korff, supra note 127, at 105.
\(^{215}\) Telephone interview with Peter Swire (Mar. 2, 2005).
\(^{216}\) The Notification of Risk of Personal Data Act, S. 1350, is pending before the Senate Judiciary Committee. Under its provisions, any person engaged in interstate commerce who owns or
requested comments on proposed rules requiring financial institutions to establish a response system, including customer notification, in the event of a security breach.\textsuperscript{217} Moreover, discovery of a database security breach may give rise to disclosure obligations under state and federal criminal laws. For example, California's Security Breach Information Act of 2003, or SB 1386,\textsuperscript{218} and other state laws have recently exposed several high profile data thefts, which are spurring consumer protection bills in Congress. In March 2005, the Senate Banking Committee held a hearing on Identity Theft,\textsuperscript{219} largely in response to widely-publicized security breaches at Bank of America and ChoicePoint, a provider of identification and credential verification services. Senator Patrick Leahy (D-VT) of the Senate Judiciary Committee has labeled these data breaches a massive threat to individuals as well as to national security.\textsuperscript{220} As of April 2005, several bills were pending in Congress that would require better subject access to data and more stringent disclosure requirements.\textsuperscript{221} On June 16, 2005, the Senate Commerce Committee held a Hearing on federal legislative solutions to data breach and identity theft, and there may be serious congressional action in this area in the near future.

In the EU, the data subject's formal right of access may not be as broad or as widely exercised as it appears from the language of the Directive. There are several important limitations on the general right of access, including a requirement that providing access not be unduly burdensome on the data controller. Furthermore, access to personal information does not include those documents in which an individual has only participated as a contributor and not a subject.\textsuperscript{222} For example, the UK Court of Appeal in \textit{Durant v. FSA} substantially limited the scope of subject access by limiting the notion of licenses electronic data containing personal information would be required, upon discovery of a breach of security, to notify any U.S. resident whose unencrypted personal information may have been acquired by an unauthorized person. In addition, H.R. 818, currently pending in the House Financial Services Committee, would amend the GLBA and the FCRA to require a financial institution to notify a consumer whose nonpublic personal information may have been compromised through unauthorized disclosure.


\textsuperscript{218} SB 1386, Gen. Assem., Reg. Sess. (Cal. 2002), entered into effect on July 1, 2003 (requires organizations that keep databases containing sensitive information on individuals to notify those individuals as well as to provide access to personal records if there is a security breach resulting in exposure of personal data).

\textsuperscript{219} Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs, 109th Cong. (Mar. 10, 2005).

\textsuperscript{220} Id. (statement of Senator Patrick Leahy (D-Vt.)).

\textsuperscript{221} Senators Charles Schumer (D-N.Y.) and Bill Nelson (D-Fla.) introduced a bill on April 12, 2005 to require better disclosure from data brokers. This bill would also create a new Office of Identity Theft at the FTC to help victims of identity theft. The Senate Judiciary Committee held hearings on April 13, 2005 regarding the Notification of Risk to Personal Data Act of 2005, a bill introduced by Senator Dianne Feinstein (D-Calif.). The bill, modeled on SB 1386, is a notification law that requires businesses to tell an individual when his private information has been compromised.

\textsuperscript{222} See, e.g., \textit{Durant v. FSA}, supra note 119.
"personal data" under the UK's Data Protection Law of 1998.\textsuperscript{223} The Court of Appeal stated that whether or not any particular information amounts to "personal data" depends on where it falls in a continuum of relevance or proximity to the data subject. Durant sought information that related not to him but to a complaint made by him to the FSA; therefore, it was not personal data, and he did not have the right to access it.

As in the United States, many European financial institutions provide customers with account records in the ordinary course of business. Data controllers are required to provide access if doing so would not require them to carry out an exhaustive search for data that could be held anywhere on their systems. However, Data Protection Authorities accept that, for large organizations, compliance with this standard would be enormously costly. Therefore, in practice, controllers are generally obliged only to carry out searches that they would carry out in the course of normal, day-to-day operations. In other words, data which would not normally be retrievable need not be provided.\textsuperscript{224}

Furthermore, Member States' differences in the substantive scope of access provided, coupled with confusion as to which State's law will be applicable, tend to preclude enforcement of the national access laws. Only some states, for example, require access to information about the sources of the data, and states differ as to the form in which information must be provided.\textsuperscript{225} Many of the national implementation laws do not provide for a "right to object," or they limit it contrary to the Directive.\textsuperscript{226} The laws in all the Member States provide for the right of data subjects to receive, on request, confirmation of whether their data is processed by a particular controller.\textsuperscript{227}

Finally, statistics demonstrate that demand for access in the EU is not substantial. According to the Commission's 2001 Inter-Active Policy Making online consultation ("IPM survey"),\textsuperscript{228} the number of access requests in 2001 was not overwhelming; out of 317 controllers who responded to the query, 65% responded either that there were less than 10 access requests or that there were no figures available. Only 25% of controllers stated that responding to access requests from individuals was an "important" effort for their organization.

To summarize, US laws provide subject access to credit and billing data, and state laws and industry practices often accommodate certain access demands. In conjunction with the EU's differential enforcement of the right of

\textsuperscript{223} Id.
\textsuperscript{224} Korff, supra note 127, at 107.
\textsuperscript{225} Id. at 105.
\textsuperscript{226} Id. at 113.
\textsuperscript{227} Id. at 107.
\textsuperscript{228} First Report on the Implementation of the Directive, supra note 108, at 9. The questionnaire includes all types of data controllers, only about 10% of which (97 out of 982) described themselves as being primarily in financial services. However, The Commission recognized that the results cannot be considered representative in the way that survey results based on a scientifically selected sample can. Furthermore, there was little information provided about the size of the data controllers or the number of total customers their access figures are based on.
access and its national limitations on the scope of access through case law and otherwise, these regulations should permit the conclusion that, if the practical rights are formalized and enforced, the right of access to personal financial data would be functionally equivalent to that provided in the EU.

C. Standards of Consumer Control Over Information Sharing

"Consumer choice" in this context refers to the ability of the data subject to control the secondary uses of personal data following its collection by a financial institution. US and EU laws differ with respect to the following issues: the requirement of purpose specification; the limit on the duration of storage; consumer choice in whether institutions can share information with affiliates; choice in whether sharing can occur with third parties pursuant to joint marketing arrangements and statutory exceptions; and the standard of consent for transfer or disclosure of sensitive data. In the EU, consumers are given broad opportunities to control data use and sharing, while in the United States consumers have very little control over the secondary uses of information by financial institutions.

First, in the EU, data generally must be processed for a specified purpose, and it may not be processed, used or transferred for that or any other purpose unless certain conditions are met to ensure that the processing is "fair and lawful." If it is used for a purpose other than that specified, the controller must have explicit authorization for such use from the data subject or the use must be necessary for some other important interest, such as performance of the contract or to serve the "vital interest" of the data subject. Although US legislation has few express requirements to specify a purpose for data collection, there are certain situations in which federal law indirectly provides that there must be a narrow purpose for data collection, such as electronic fund transfers and collection of information by a credit card issuer for billing purposes. Furthermore, most banks have internal policies mandating confidentiality of customer records and thus may limit external secondary uses of information. While the US lacks specific legal rights that restrict the collection of unnecessary payment transaction data, most financial institutions usually do not collect information beyond the data needed to execute and confirm payment.

In addition, in the EU, despite the fact that Member States uniformly use the purpose-specification and use-limitation language of the Directive, the inherent flexibility of the principles leaves them open to divergent application, and Member States apply different tests. For example, in determining "incompatible use," Member States' laws range from the "reasonable expectations" of the data subject, to "fairness," to the application of various

229. SCHWARTZ & REIDENBERG, supra note 3, at 268.
230. Id. at 271.
231. Id. at 273.
"balance" tests. Several Member States have more general, relaxed rules which allow for processing whenever "authorized by law" or by "special provisions" under any law. A recent Eurobarometer Survey indicated that there is a generally low level of compliance with regard to providing data subjects with "the purpose of the processing for which the data are intended."

Second, in contrast to the EU, the US does not have general laws limiting the duration of storage for personal information, but there are limits on dissemination of credit information by a Credit Reporting Agency following statutorily defined periods of time. Generally, there are minimum retention periods imposed on financial institutions for electronic fund transfers or credit card transactions because financial institutions would otherwise dispose of transaction records as quickly as necessary to serve corporate interests. The EU also imposes such retention requirements for financial services providers. As a result, firms in compliance with the applicable financial regulations may be in violation of the Directive. Recently, proposed requirements for online data retention have been strongly advocated by several states.

Third, consumers do not have the right to prevent US financial institutions from sharing certain information with affiliates, while consumers may opt out of transfers to affiliates in the EU. Although the FCRA requires that consumers be given notice and the opportunity to opt-out of affiliate sharing with respect to eligibility information, the GLBA does not limit such sharing with respect to experience information. However, in the EU, due to different corporate conglomerate structures such as universal banks, data protection laws may permit free sharing between different parts of a company that would technically be "affiliates" under US law. Thus, the US standard may in practice be similar to the European standard because "affiliates" in the US are the analogues of divisions of the same company in the EU. David Aaron, Undersecretary of Commerce for International Trade, stated in congressional testimony:

The European banking institutions and financial institutions aren't structured the way we are. They have insurance. They have brokerage. They have banks. They are not affiliates. They are actual divisions of a company. So, therefore, they share this between each other all the time, with no difficulty. We are structured—many of our companies are structured differently. So all of a sudden you get this issue of affiliate sharing, and whether there should be opt-in or there should be opt-out. Well, I think we have got to be careful there because the fact

233. Id. at 10.
235. SCHWARTZ & REIDENBERG, supra note 3, at 274.
236. Id. at 296.
237. Id. at 274-75. However, marketing departments may retain personal information for longer periods for the purpose of studying long-term personal habits.
of the matter is if we accepted either one of those procedures—and we did accept opt-out to some extent—we find ourselves at a competitive disadvantage.241

However, universal banks generally do not include the broad range of “financial activities” that financial holding companies in the US may include under the GLBA. In addition, consumers may not expect sharing between different companies, even if they happen to be affiliates, while customers would expect sharing within a universal bank. With the passage of the GLBA in 1999, it was expected that many of the affiliates that had been kept separate by regulation would merge, and it was implicitly understood that consumers would expect such services to come from the same organization. Representative Michael Oxley (R-Ohio) stated at a Congressional Hearing on the GLBA that “the integrated products and services today’s consumer expects from his or her financial institutions require information sharing, especially among affiliates. After all, in the eyes of the consumer, what are affiliates other than different departments of the same company that they are dealing with.”242 Thus, the affiliate choice distinction between the US and the EU may not be as significant as it appears. However, there may still be a difference in the sense that affiliate sharing may occur in the United States between entities that would not be permitted to be under the umbrella of a universal bank.

Fourth, while the GLBA prohibits financial institutions from disclosing account numbers to nonaffiliated third parties for marketing use,243 the consumer does not have the choice to object to information shared with a “joint marketing” partner. However, if such “joint marketing” occurs, the contractual agreement requires the third party to maintain the confidentiality of such information.244 This exception to the opt-out requirement was originally based on the idea that a principal should be able to choose whether to hire an employee or an independent contractor to perform a task.245 Similarly, the EU’s Directive provides for a “data processor” that is the analogue of the US’s “joint marketing partner.” However, the Directive places greater constraints on the contractual relationship between the controller and his agent, as described below.246

The “chief problem” of the joint marketing exception has been described as the fact that the third-party marketing partner is technically permitted to use the information it receives freely for its own purposes and within its own family of affiliates.247 However, in practice, many joint marketing agreements limit the use of the data to those purposes for which it is disclosed. In December 2001,

245. Swire, supra note 22, at 1297.
247. Swire, supra note 22, at 1301.
staff of the federal banking agencies issued a series of Frequently Asked Questions (FAQs) clarifying how banks can qualify for the joint marketing exception, in particular for products such as insurance and annuities.\textsuperscript{248} Under these guidelines, the bank’s written agreement with the nonaffiliated company to jointly offer, endorse or sponsor a financial product or service must (a) restrict the insurance company from disclosing or using customer information for any purpose other than selling insurance products to the bank’s customers and (b) comply with the banking agencies’ customer information security guidelines.\textsuperscript{249} Moreover, the FAQs specify that a bank’s initial privacy notice must include a separate statement describing the joint marketing arrangement.\textsuperscript{250} Currently, large financial institutions often fail to disclose the details of the extent of the sharing or the partners’ identities.\textsuperscript{251} The GLBA also precludes third-party recipients from sharing information pursuant to a joint marketing agreement, thus precluding a chain of third-party joint marketing agreements.

Under the EU standard for disclosures of information between controllers and processors, a processor who has access to personal data must not process such data except on instructions from the controller,\textsuperscript{252} and the controller must guarantee the security of the processing.\textsuperscript{253} The Directive’s Article 17 provides more detailed legal contractual requirements than the GLBA’s requirement of maintaining confidentiality; it provides that the controller must supervise the processor’s guarantees of technical security and organizational measures and ensure compliance.\textsuperscript{254} In addition, in several Member States, the controller is liable for the (wrongful) actions of the processor.\textsuperscript{255}

However, in Europe, there may be difficulties enforcing the rules with respect to data processors due to uncertainty as to the applicable governing law. The law that applies to the processor should in theory be the law of the country in which the controller is situated. However, the processor must adhere to his local law as far as the legal requirements concerning security and confidentiality are concerned. Finally, the law of the contract between the controller and the processor covers, \textit{inter alia}, the respective liabilities towards one another. As a result, various national laws may apply, which “makes for a very complex

\begin{itemize}
\item \textsuperscript{249} Financial Services Modernization 2003: Implementation of the Gramm-Leach-Bliley Act, A.L.I.-A.B.A. COURSE OF STUDY MATERIALS, Feb. 2003. Examples of an agreement that jointly offers, endorses or sponsors a financial product or service would be an agreement in which the insurance company agrees to use the bank’s name in its marketing materials or an agreement where the insurance company agrees to offer insurance products and services on the bank’s premises.
\item \textsuperscript{250} \textit{Id.}
\item \textsuperscript{251} Swire, \textit{supra} note 22, at 1321.
\item \textsuperscript{252} Data Protection Directive art. 16.
\item \textsuperscript{253} \textit{Id.} art. 17.
\item \textsuperscript{254} \textit{Id.} art. 17(2).
\item \textsuperscript{255} Korff, \textit{supra} note 127, at 158.
\end{itemize}
In sum, the controller in the EU is legally required to exercise greater control over the information shared than the US institution that discloses information to a partner under a joint marketing agreement. In practice, US agreements that follow the FAQs’ guidelines may limit the scope of the service provider or partner’s use of the information.

Fifth, the generally accepted statutory exceptions under which consumers may not prevent information sharing are similar in the GLBA and in the Directive. The GLBA provides that transfers may be carried out without notice “as necessary to effect, administer or enforce a transaction requested or authorized by the consumer”; the Directive provides that processing is lawful if it is “necessary for the performance of a contract to which the data subject is party.” In both the US and the EU, the data subject implicitly consents to any processing that is necessary. However, the EU subjects international transfers to further scrutiny under Article 25.

The United States and the European Union also have similar provisions to allow processing in order to protect the data subject’s interests or when necessary to comply with a legal obligation. One real difference in the statutory exceptions is that the EU makes processing lawful when necessary for the performance of a task carried out “in the public interest,” thus providing a broader exception than exists under US law. Another difference is that the United States has additional exceptions for transfers in connection with sales, mergers, transfers, or exchanges of business or operating units, as well as for providing information to insurance rate advisory organizations and auditors. These exceptions are for corporate activities that are unlikely to harm individuals.

Finally, while the EU Directive provides that processing is lawful if the data subject has “unambiguously given his consent,” the GLBA provides explicitly for an opt-out standard, thus creating a potential gap between implicit and explicit authorizations. However, national Data Protection Authorities permit opt-out systems in practice, reserving the strictures of the opt-in only for sensitive information. The Directive does not specify the form in which consent must be obtained, and there is not widespread consensus on the

256. Id. at 162.
258. Data Protection Directive art. 7(b).
261. Data Protection Directive art. 7(e).
263. Data Protection Directive art. 7(a).
265. Confirmed by Rosa Barcelo, supra note 190.
opt-out versus the opt-in among the Member States.\textsuperscript{266} Because of the tremendous costs to financial institutions and society associated with the opt-in regime, Cate and Staten asserted, "'[o]pt-in' may be the law on the books throughout Europe, but 'opt-out' is the reality because government officials realize the blow that an 'opt-in' requirement would deal to European economic performance."\textsuperscript{267} Given that the FCRA also uses an opt-in standard for sensitive credit data, the standard of choice distinction (opt-in versus opt-out) may be largely illusory.

Furthermore, even though the GLBA only requires opt-out, some states have adopted opt-in standards.\textsuperscript{268} The difficulty with stricter state legislation regarding affiliate sharing is that it may be preempted by the FCRA's affiliate sharing opt-out provisions. However, a recent decision upholding more stringent state privacy legislation in California against the FCRA's preemption provisions may open the door to increased state privacy regulation. In \textit{ABA v. Lockyer},\textsuperscript{269} the Court found that because the FCRA preemption provision only relates to consumer reports, it does not broadly preempt all state laws regulating sharing of other types of information by affiliates. "Limitations on the sharing of personal financial information between financial institutions in non-credit reporting situations are specifically contemplated by the provisions of the GLBA, which allows states to enact more stringent privacy regulations in that regard, therefore permitting state laws like SB1."\textsuperscript{270} The industry groups have filed an appeal to the Ninth Circuit.\textsuperscript{271}

In sum, the most significant differences between the actual choices that

\textsuperscript{266} Charlesworth, \textit{supra} note 195, at 943.
\textsuperscript{268} States that have opt-in regimes include North Dakota, California, Vermont, Alaska, Connecticut, and Illinois. Alaska generally requires customer consent for a financial institution to disclose customer information, with no blanket exception or authorization for sharing information. A Connecticut law similarly requires consent for disclosure by financial institutions subject to certain exceptions, but it contains no blanket exception for sharing of information among affiliates and places restrictions on sharing of information with broker-dealers. North Dakota requires customer written consent for sharing of information among affiliates. Vermont's prohibition of information sharing does not contain an exception for inter-affiliate sharing of customer information. \textit{See Privacy Protection for Customer Financial Information}, CRS Report RS20185 (updated Jan. 5, 2001).
\textsuperscript{269} American Bankers Ass'n v. Lockyer, 2004 U.S. Dist. LEXIS 12367 (E.D. Cal. June 20, 2005) (upholding California's SB 1, also known as the California Information Privacy Act, \textit{CAL. FIN. CODE} § 4050 (2004), which took effect July 1, 2004).
\textsuperscript{270} \textit{See id.}\ See also \textit{Federal Court Rules California Privacy Statute Takes Precedence Over FACT Act}, 28 EFT REPORT 14, 19-20, 2004 WL 62675944 (July 7, 2004).
\textsuperscript{271} \textit{See Am. Bankers Ass'n, supra} note 269. Some commentators predict that this decision will be overturned, pointing out that it is directly opposed to the "clear and unequivocal preemption provisions in the 1996 and 2003 amendments" to the FCRA in the Reform Act and the FACT Act, as well as the broad scope of preemption provided for by the U.S. District Court for the Northern District of California in \textit{Bank of America v. City of Daly City}. In the interim, the financial services industry may experience the disruptions the FACT Act's preemption provisions were designed to avoid. Fischer and Ireland, \textit{Federal Court Made Mistake In Calif. Data-Sharing Case}, \textit{CALIFORNIA}, Aug. 2004.
consumers have in the EU and the US are the EU citizens’ formal right to purpose-specification at the initiation of the customer relationship and certain safeguards assured by the Directive in the context of joint marketing or contracting with service providers. The US opt-out is currently very similar to the EU provision for obtaining consumer consent, except that sensitive data may use a different standard. Finally, the affiliate sharing provisions may not be as significant as they initially appear because of the realities of European financial practices, but there may still be some discrepancies.

D. Treatment of Sensitive Information

Pursuant to Article 8(1) of the Directive, many EU Member States’ laws create more stringent opt-in policies for sharing data relating to racial or ethnic origin, religious beliefs, sex life, or trade union memberships. While the GLBA does not provide for special treatment of sensitive data, the FCRA includes an opt-in standard for use of sensitive data in credit reports, such that US protection of sensitive credit information has been described as “functionally similar” to that in the EU.\(^{272}\) The FCRA places greater restraints on disclosure or use by CRAs of information relating to criminal records, sex, race, ethnic origin, age, or marital status.\(^{273}\) In addition, the Equal Credit Opportunity Act\(^{274}\) and similar state discrimination statutes prohibit discrimination against individuals on the basis of race, color, religion, national origin, sex, marital status, age, or because an applicant receives income from a public assistance program. Employing a broad definition of “sensitive,” the ECOA and FCRA limit the uses to which sensitive information can be put. Sensitive data is considered “sensitive” because it is more personal and therefore can cause more harm to individuals if misappropriated. Under this logic, the United States protects sensitive data where abuses are most likely to occur, as in the context of discrimination. In practice, sensitive data collection may not even be necessary for the performance of many financial services.

In addition, the FACTA specifically allows consumers to prevent affiliates from sharing consumer reports that include medical data.\(^{275}\) Except for insurance transactions, the FACTA requires financial institutions to obtain specific written consent that includes a clear and conspicuous description of the use for which the agency is disclosing the medical information.\(^{276}\) It restricts creditors from obtaining or using medical information from an affiliate and

---

272. SCHWARTZ & REIDENBERG, supra note 3, at 303.
273. See id.
275. Title IV of FACTA. Specifically, the FACTA makes the standard exclusions from the definition of “consumer report” inapplicable if medical-related information is contained in the disclosure, so that any medical information shared by affiliates will be considered a consumer report. Medical information is defined in section 603(i) of the FCRA as information or data, other than age or gender, relating to past, present or future physical, mental or behavioral health, the provision of health care to an individual or the payment for the provision of health care to an individual.
using it in determining the consumer's credit eligibility, subject to certain exceptions for insurance and other circumstances specifically exempted by the federal banking agencies and the NCUA and FTC. The federal banking agencies issued a notice of proposed rulemaking regarding these provisions of the FACTA on April 28, 2004, allowing banks, thrifts, and credit unions to use medical information in a credit decision when "necessary and appropriate" in connection with determinations of consumer eligibility for credit.

However, in the non-credit context, sensitive data is subject to more stringent protection in the European Union than in the United States. According to the Directive, the processing of "special categories of data" must be prohibited by Member States unless the data subject gives "explicit consent." The Directive gives Member States the option to provide that data subjects not be permitted even to consent to processing of their sensitive data. Some countries lay down strict "necessity" tests or require that controllers obtain special permits or authorizations. Several DPAs defer to other domestic laws or rules that authorize sensitive data processing, as permitted by Article 8(4). However, under Article 8(4), these exceptions must be subject to provisions providing for adequate safeguards, yet some Member States have not adopted such safeguards, and, to the extent they exist, they are often unsatisfactory. The Commission has not always been notified of alternative national laws governing sensitive data, and therefore it is difficult to determine the extent to which they undermine Article 8's provisions.

In sum, differential treatment of sensitive data in the United States and the European Union outside of the credit context appears to stem from different ideologies: in the European Union, data protection preserves a fundamental human value inherent in private life, while in the United States, it is protected to prevent abuse and discrimination. It may be that the European rules surrounding sensitive personal data are at times unnecessarily strict when viewed in the context of the actual risks posed to individuals. The functional difference seems to represent a philosophical difference in the conception of privacy and

278. Damian Paletta, As Deadline Nears, FACT Rules & Far From Done; Fair and Accurate Credit Transactions Act, AM. BANKER, October 25, 2004. For example, one exception in the proposed rule would allow a creditor to obtain and use medical information that pertains to debts, expenses, income, benefits, collateral, or the purpose of the loan. Another exception would allow lenders to obtain medical information needed to verify the purpose of a loan sought to finance a medical procedure or purchase medical equipment. Also, a financial institution could obtain medical information needed to comply with local, state or federal laws or to prevent or detect fraud.
279. Data Protection Directive art. 8(2).
280. Id. art. 8(2)(a).
281. Korff, supra note 127, at 82.
283. Korff, supra note 127, at 82.
the purposes it is meant to serve. It is one area where compromise may be necessary.

E. Enforcement

EU privacy protection relies on principles embodied in law and a system of "external supervision" by an independent authority. However, the European Commission has stated that these two features are not necessarily required for protection to be considered "adequate." The Article 29 Working Party has stated that the objectives of a data protection procedural system are essentially threefold. First, the procedure must deliver a good level of compliance with the rules. Second, it must provide support and help to individual data subjects in the exercise of their rights, such that the individual can enforce his or her rights rapidly and effectively, without prohibitive cost. This requires an institutional mechanism allowing independent investigation of complaints. Third, the procedure must provide appropriate redress to the injured party if rules are violated. This should involve a system of independent arbitration which allows compensation to be paid and sanctions imposed where appropriate.

This section will consider enforcement mechanisms and policies in light of these three requirements. In the US, a variety of federal and state agencies, as well as self-regulatory practices, are responsible for ensuring that privacy protections are enforced. Although compliance and enforcement statistics are difficult to obtain because the federal agencies do not separate privacy enforcement actions from enforcement of other rules, there appear to be generally high levels of compliance with existing laws. There is also institutional support for data subjects. Effective redress for damages may often be pursued through state laws. In the EU, enforcement statistics for the financial sector were also very difficult to find because they are located in 25 different DPAs, and they are not divided up by sector. Enforcement generally occurs through the supervisory DPAs in the Member States, focusing on individual data subjects' rights to redress. While there is little comprehensive data on compliance, studies have shown divergent Member State implementation, as well as inadequate enforcement resources. The DPAs are the primary institutional mechanisms, and it is through them that individuals receive support and redress. While there are sanctions and criminal penalties for violations, these are rarely used because compliance can be achieved through negotiation and consultation with the DPA.

It has been suggested in congressional testimony in the United States that "[u]nlike the EU’s lax enforcement of its privacy directive, the U.S. systematically enforces its privacy laws." Professor Fred Cate, in his testimony at the Senate Hearing on Financial Privacy in September 2002, stated

286. Id.
287. 107th Cong. 98, supra note 241 (statement of Jonathan M. Winer, Alston & Bird, LLP).
that "there is virtually no evidence of tangible harms to consumers that are not already covered by Gramm-Leach-Bliley, the Fair Credit Reporting Act, or some other financial privacy law."\footnote{288} Moreover, Minnesota Attorney General Mike Hatch stated that the GLBA’s customer protections have proven "of little value" in protecting consumers, and as proof he offered that "[a]ll 50 State Attorneys General recently filed comments with the FTC stating that consumer complaints and State consumer protection enforcement actions against preacquired account telemarketers have continued without significant change after passage of the GLBA."\footnote{289} Attorney General Hatch’s office has continued to bring actions for telemarketing schemes after the passage of GLBA.\footnote{290}

1. Enforcement in the United States

In the United States, there appears to be a relatively good level of compliance among the regulated financial institutions. A 2002 study on whether or not to impose new regulation of the commercial market for personal information found that, "despite perceptions to the contrary, there is a striking lack of evidence of consumer harm from privacy violations associated with the commercial use of information for advertising and marketing purposes."\footnote{291} The federal regulatory agencies responsible for ensuring compliance with the GLBA and the FCRA describe themselves as "active in protecting financial privacy."\footnote{292} Recently, the FTC has enforced its Safeguards Rule\footnote{293} against mortgage companies in a nationwide compliance sweep enforcing the Safeguards Rule.\footnote{294} The FTC also actively monitors compliance with the adverse action notification provision of the FCRA.\footnote{295}

\begin{itemize}
  \item \footnote{288}{107th Cong., supra note 67 (testimony of Professor Fred Cate).}
  \item \footnote{289}{Id. (testimony of Mike Hatch).}
  \item \footnote{290}{See Minnesota v. Fleet Mortgage Corp., 158 F. Supp. 2d 962 (D. Minn. 2001); Minnesota v. Fleet Mortgage Corp., 181 F. Supp. 2d 995 (D. Minn. 2002). See also complaint filed by the State of Minnesota against Fleet Mortgage, December 28, 2000, available at http://www.ag.state.mn.us/consumer/news/pr/CompFleet122800.html. Fleet Mortgage Corporation entered into contracts in which it agreed to charge its customer-homeowners for membership programs and insurance policies sold using pre-acquired account information. If the telemarketer told Fleet that the homeowner had consented to the deal, Fleet added the payment to the homeowner’s mortgage account.}
  \item \footnote{291}{PAUL H. RUBIN AND THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 83 (2002).}
  \item \footnote{292}{Howard Beales, Director, Bureau of Consumer Protection, FTC, Remarks: Privacy Notices and the FTC’s 2002 Privacy Agenda (Jan. 24, 2002).}
  \item \footnote{293}{See 67 Fed. Reg. 36,484 (May 23, 2002).}
  \item \footnote{294}{Administrative actions were filed against Nationwide Mortgage Group, Inc. and its president, based in Fairfax, Virginia, as well as Sunbelt Lending Services, Inc., based in Clearwater, Florida. Sunbelt has settled the charges brought pursuant to the FTC’s Safeguards and Privacy Rules (16 C.F.R pt. 313 and 16 C.F.R pt. 314) and section 5(a)(1) of the FTC Act in an FTC Decision and Order dated January 3, 2005, http://www.ftc.gov/os/caselist/0423153/050107do0423153.pdf (the consent order bars Sunbelt from future violations of the Safeguards Rule and the Privacy Rule and sets out requirements for its security program to be certified within six months and biannually thereafter by an independent professional).}
  \item \footnote{295}{Remarks of Howard Beales, supra note 292.}
\end{itemize}
Comptroller of the Currency (OCC) is committed to policing privacy violations by the banks under its jurisdiction. Although a source within the OCC confirmed that there have not been a large number of actions,\textsuperscript{296} the agency takes its responsibility seriously.

The federal regulators frequently issue guidelines with respect to financial privacy protections. Virtually all of the regulators charged with implementing the legislation have provided not only regulations but also FAQs, Guidelines, and other information and resources to ensure effective application of the laws.\textsuperscript{297} The FTC and the seven financial regulatory agencies are taking measures to improve notices, such as hosting GLBA notice workshops.\textsuperscript{298} Furthermore, the OCC and other federal banking agencies have issued uniform examination procedures to verify compliance with the implementing regulations, including requirements regarding privacy and opt-out notices, reuse and redisclosure of nonpublic personal information, and account number sharing.\textsuperscript{299} The Banking Agencies have jointly issued guidelines implementing the security standards contained in Section 501(b) of the GLBA ("Security Guidelines").\textsuperscript{300} The OCC has also issued advisory letters regarding information sharing.\textsuperscript{301} In addition, there may be significantly higher levels of enforcement of financial regulations in the United States than in the European Union, and it is reasonable to assume that such levels of intensity would extend to privacy regulation as well.

Support for individuals in exercising rights of information privacy in the financial sector is provided in the United States through the GLBA and FCRA notices as well as through self-regulatory codes of conduct adopted by financial institutions, often pursuant to federal guidelines. Furthermore, strong privacy advocacy groups such as the Electronic Privacy Information Center ("EPIC"), the Privacy Rights Clearinghouse, and the US Public Interest Research Group are influential in calling media attention to privacy violations and assuring that consumers are aware of their rights.\textsuperscript{302} In practice, many banks state their privacy policies clearly and provide click-through or telephone mechanisms that make it easy for customers to opt out.\textsuperscript{303}


\textsuperscript{297} For example, in 2002 the FTC released FAQs to assist with compliance with the GLBA and on December 12, 2001, the federal banking agencies issued guidance to help financial institutions comply with the regulations, http://www.ftc.gov/privacy/glbact/glb-faq.htm.

\textsuperscript{298} Remarks of Howard Beales, \textit{supra} note 292.


\textsuperscript{300} See 66 Fed. Reg. 8,616 (Feb. 1, 2001).


Although many claim that the opt-out notices provided to customers in the United States pursuant to the GLBA have in practice failed to provide consumers with effective choice, the federal banking agencies have issued regulations and are currently making efforts to remedy this shortcoming. The notices were criticized as incomprehensible, and reports indicate that most are written at a college upperclassman reading level. A Petition for Rulemaking filed by Public Citizen requested improvements in the clarity of notices and the ease of opting out, demanding that federal agencies require a standardized notice that clearly explains consumers' rights. The federal agencies have responded. In December 2003, the eight federal agencies issued an Advance Notice of Public Rulemaking to consider the development of alternative forms of privacy notices for consumers, soliciting public comments on the feasibility, design, and content for a short notice. The agencies are currently engaged in an interagency notice research project to develop alternative forms of privacy notices through consumer testing.

Perhaps the single greatest obstacle to creating a comprehensive privacy enforcement regime in the US financial services industry is the problem of uniting and coordinating multiple regulatory agencies with overlapping jurisdictional mandates. Coordination is further complicated in that financial institutions may face an extra layer of stricter state regulation, which may or may not be preempted.

With respect to individual remedies and causes of action, US consumers must obtain redress from explicit legal rights provided by other state and federal laws, such as the GLBA and the FCRA, rather than from legislation governing financial institutions, which provide for actions to be initiated only by federal regulatory agencies. However, individuals may have claims for financial privacy violations pursuant to other federal statutes, such as the EFTA or the ECOA. Furthermore, individual redress is also provided by state fund transfer regulations and computer crime laws, as well as state law contract and tort claims.

307. 68 Fed. Reg. 75,164 (comments were due Mar. 29, 2004).
308. The agencies have issued a “Statement of Work: Form Development Project,” describing the research design for the first “form development” phase of the project and hired a contractor to begin form development and testing, available at http://www.ftc.gov/privacy/glbact/sow_privacy_notice_final1.pdf.
310. 15 U.S.C. §§ 1693(m),(n) (2006) ((m) is civil liability, (n) is criminal liability).
312. SCHWARTZ & REIDENBERG, supra note 3, at 283.
The GLBA specifically preserves state remedies for individuals, including unfair practice claims. Voluntarily adopted privacy policies, such as the ABA's adopted Privacy Principles,\(^{313}\) can often result in legally enforceable consumer rights under state law. Various common law tort claims are based on a reasonable expectation of privacy, and stated policies create expectations. Furthermore, breach of a privacy policy could be deemed an "unfair or deceptive act" under the FTCA.\(^{314}\) In addition to banks' common law obligations of confidentiality, all states have laws providing consumers with a state right of action to remedy unfair or deceptive practices. States themselves can also bring suits for violations of state and federal law.\(^{315}\) Class action lawsuits may also be effective where an institution has committed violations that affect a large number of individuals.

Personal data protection in the insurance field is enforced by 51 different state authorities. However, while insurance companies are generally in compliance with the GLBA's notice requirements, most State regulators have not yet implemented security and confidentiality requirements.\(^{316}\) Enforcement of security measures thus may occur pursuant to the provisions of the previous NAIC Model Act of 1982, which offers significant protections.

2. Enforcement in the European Union

The overall level of compliance is difficult to measure in the European Union because it differs widely between the 25 regulatory bodies of the Member States. National Data Protection Authorities have different enforcement programs and priorities and are endowed with varying enforcement powers and resources.\(^{317}\) The Working Party has been charged by the Commission to hold periodic discussions on enforcement and to launch sectoral investigations at the EU level in order to provide a more accurate picture of the implementation and enforcement of data protection law in the Community.\(^{318}\) In 2004, the Working Party stated that the promotion of harmonized compliance is one of its strategic and permanent goals.\(^{319}\) The Working Party has committed itself to developing proactive enforcement strategies, such as awareness-raising activities and guidance, increasing enforcement actions such as sanctions, and intensifying its cooperation efforts through mutual assistance.\(^{320}\) The Working Party has also

---

313. See supra note 87.


315. See, e.g., Fleet Mortgage Corp., supra note 294.

316. GAO Report, GAO-02-361, supra note 26, at 3.


called for investigations of the enforcement practices of the national DPAs.\footnote{321}{In early 2005, the Working Party will develop a list of candidate issues, cases or sectors and will determine their eligibility for EU-wide synchronized national investigations to be undertaken in 2005 and 2006, with due regard to the diversity that exists in terms of the powers, policies and resources of national DPAs. \textit{Id.}}

In 2003, the First Report on the Implementation of the Data Protection Directive\footnote{322}{\textit{First Report on the Implementation of the Directive, supra note 108.}} found that it was difficult to obtain accurate or complete information about compliance with the data protection laws. Anecdotal evidence, combined with various elements of "hard" information available to the Commission, such as the small number of individual complaints received by the Commission itself and the low number of authorizations by national DPAs for transfers to third countries notified to the Commission in accordance with Article 26 (3), were taken to suggest the presence of three interrelated phenomena.\footnote{323}{Id. at 12.}

First, the enforcement effort is under-resourced and supervisory authorities are charged with such a wide range of tasks that enforcement actions have a low relative priority. Second, data controllers may be reluctant to undertake changes in their existing practices to comply with what may seem to be complex and burdensome rules when the risks of getting caught seem low. Third, data subjects demonstrate an apparently low level of knowledge of their rights.\footnote{324}{Id.} The DPAs themselves in many Member States are particularly concerned about their DPAs' lack of resources.\footnote{325}{Id. at 17.}

Several obvious problems with enforcement stem from divergent implementation in various Member States. For example, Article 4's "applicable law" provisions have been inconsistently implemented, thus subjecting data controllers in the EU to the regulations of several sets of national laws simultaneously and creating great confusion as to which laws should be followed and enforced. Submissions to the Commission from Member States on the occasion of its first implementation report argued for a country of origin rule that would allow multinational organizations to operate with one set of rules across the EU. Many also argued that the "use of equipment" was not an appropriate or workable criterion for determining the application of EU law to controllers established outside the EU.\footnote{326}{Id.} In the 2002 survey conducted by Interactive Policy Making (IPM) for the European Commission, 32\% of the respondent data controllers believed that the disparities between Member States' legislation were too significant to consider that data can be moved freely within the Community/EEA. Fifty percent of the respondents believed that data protection supervisory authorities did not devote sufficient resources to advising companies.\footnote{327}{Questionnaire for Data Controllers on the Implementation of the Data Protection Directive (95/46/EC): Results of Online Consultation 20 June - 15 September 2002, Study Conducted by Interactive Policy Making (IPM).}
With respect to support for individuals in enforcing their rights, "notice" to consumers in the EU appears to occur with "purpose specification" at the initiation of the relationship; the individual consents to processing for a particular purpose. Awareness of data protection rights varies immensely between Member States. David Smith, Assistant Information Commissioner from the UK, stated, on behalf of the UK's Commission, "We are very keen to develop awareness amongst citizens and amongst businesses of how the law operates and their rights and responsibilities under it." According to the other IPM survey for data subjects, the largest single category of respondents (4113 out of 9156, or 44.9%) considered the level of protection in the EU at a minimum, and 81% of individuals thought the level of awareness about data protection was insufficient, bad or very bad. Of the controllers, the largest single group, 295 of 982, responded that citizens' awareness of data protection was insufficient. Most believed that the existing data protection requirements are necessary in a market where there is traditionally a high level of protection for consumers and a strong concern for fundamental rights. Europeans are increasingly aware of personal data protections, and, for example, they are becoming more skeptical about giving broad consent to controllers to transfer data to third countries.

The UK data controllers' responses to a Department of Constitutional Affairs consultation in 2002 suggest that they have received more subject access requests under the 1998 Data Protection Act than under the previous 1984 Act.

Finally, the EU provides that data subjects must have judicial remedies and rights to recover damages for breaches of national data protection laws. The Commission or the Council may also challenge the adequacy of Member States' laws in the ECJ, which may find Directive provisions to be directly applicable to data subjects. For example, in the UK, individuals can enforce their rights in court. As David Smith stated, "[t]he UK laws, as it stands at the moment, only allows individuals to bring cases. And I think it's fair to point out that actually the individuals' rights are fairly limited, in that it only enables them – in terms of getting redress, to get compensation for damage, which in UK legal terms involves some sort of financially quantifiable loss. And most of the data protection breaches result in distress to individuals, but not necessarily a

---

328. Statement of David Smith, Assistant Information Commissioner from the United Kingdom, supra note 241, at 16.
333. See, e.g., Case C-465/00, supra note 178.
financially quantifiable loss." A private right of action for data protection breaches is not necessarily guaranteed in the United States.

A final factor to be considered in determining levels of privacy protection is actual practice in each jurisdiction. Although empirical data is often difficult to obtain and voluntary practices are not necessarily backed by legally enforceable provisions or formal legal records, the actual practices contribute to a more comprehensive picture of the system as a whole. In the United States, financial institutions generally adhere to industry codes that bring their privacy practices in line with high consumer expectations, in part because consumers may choose to do business only with financial institutions with strongly enforced privacy policies. Furthermore, firms may also voluntarily implement more restrictive privacy policies than required by the GLBA because of the threat of more stringent state regulation that would give rise to costly changes in internal procedures to comply with state laws. Finally, privacy violations can create high-profile scandals that generate significant negative publicity.

For example, nine of the top fifteen U.S. banks, or 60%, do not share customer information with third parties, according to Financial Insights data. A research analyst with Financial Insights stated: "A lot of banks are adopting the most conservative privacy policies possible. They're not just following Gramm-Leach-Bliley guidelines, they're going even further and just not sharing data with third parties at all." Furthermore, practices reflect the fact that many consumers realize that "the abundance of marketing information out there contributes to the identity theft problem." For example, SunTrust Bank has long enforced policies of sharing and safeguarding customer information that are stricter than required by law. The only other firm SunTrust shares customer data with is its affiliate card issuer, and customers are explicitly made aware that if they choose not to share their information, they cannot get a credit card through SunTrust.

In the EU, the Commission's and the Working Party's willingness to recognize sectoral codes of conduct and binding corporate rules may indicate that certain sectors and companies are also adopting certain privacy practices voluntarily. David Smith of the UK Commission stated: "We promote good practice which goes wider than simply complying with the law and covers conduct which is consistent with those requirements ... we also put emphasis

335. Id. at 28.
338. Id. (quoting Sophie Louvel).
339. Id.
340. Id.
341. Id.
on the development of codes of practice, codes that develop how the law applies in the area of particular industry, particular activities, fields such as the use of data in employment.\(^3\)

It is likely that EU institutions respond to the same or greater privacy concerns of European consumers and adapt their policies accordingly. The traditional sector-specific bank secrecy and confidentiality norms do not generally recognize national borders. It may be that industry codes are more indicative of actual practices than the formal laws themselves.

In sum, US privacy protections appear to have generated a good level of compliance. There are many regulations and guidelines issued in response to perceived shortcomings, and relatively few enforcement actions. US regulation provides for support through a notice-based system, reinforced by self-regulatory codes and the vigilance of active consumer privacy groups, and it provides for individual redress at the state level and for most quantifiable consumer harms. In the EU, compliance with the Directive appears inconsistent, and, while there is a private right to a judicial remedy, there are indications that data subjects’ awareness levels are low. Furthermore, the judicial remedy may be limited to measurable damages, as it is under US state law. The formal legal enforcement remedies in the Directive thus in practice may be functionally equivalent to those in the United States, even if the United States lacks certain institutions or procedures that Europeans favor. The EU should acknowledge US self regulation within the rubric of compliance, support, and redress.

V.
THE EC DATA PROTECTION DIRECTIVE AND TRANS-ATLANTIC DATA TRANSFERS

Article 25 of the Data Protection Directive limits transfers to non-EU countries that have not been found to provide adequate protection;\(^3\) however, as discussed above, Article 26 permits transfers to such third countries under certain circumstances, such as when the data subject has consented or when the transfer is necessary for the performance of a contract between the data subject and the controller. In 2000, the European Commission and the Article 29 Working Party reviewed the recent US privacy legislation contained in the GLBA to assess whether it could be considered adequate for the purposes of issuing an adequacy decision. The European Parliament found that “there is not at present any generally applicable legal data protection in the private sector and virtually all data are currently processed without specific guarantees of judicial protection.”\(^3\) However, the European Parliament noted that there were

\(^3\) Statement of David Smith, \textit{supra} note 328, at 16.

\(^3\) Outside the EU, data may be transferred freely to Switzerland, Canada, Argentina and the UK territories of Guernsey and the Isle of Man, whose privacy regimes have been recognized by the Commission as offering adequate data protection. In addition, some Member States have open transfer provisions regarding transfers to non-EU EEA countries (Norway, Liechtenstein and Iceland).

numerous legislative proposals pending before Congress, that the President and the FTC supported further legislative measures, and that the guidelines approved by the OECD must in any case be applied in the area of personal data protection.\(^\text{345}\) John Mogg, Director General of the Internal Market Directorate General, indicated in 2001 that the adequacy of the GLBA was a closed issue.\(^\text{346}\)

The Commission and the US Treasury engaged in an active dialogue regarding a potential adequacy decision until 2002, when the Commission indicated that it would favor extending the Safe Harbor to financial services by adding the SEC and the federal banking agencies to the list of enforcement bodies rather than by issuing an adequacy decision regarding a given law (such as the GLBA alone). The United States held back, preferring to consider other options. Since 2002, the Treasury Department has not stated its position, nor has it sought an adequacy decision based on other legislation. The European Commission is willing to have more productive and active discussions on this topic if the US Treasury Department shows an interest in pursuing the dialogue.\(^\text{347}\) In the meetings of the Trans-Atlantic Financial Markets Regulatory Dialogue in 2005, the data protection issue was noted, but it was not discussed actively.\(^\text{348}\)

The most probable explanation of why the harmonization of Data Protection regimes is not currently at the forefront of these discussions is that Data Protection Authorities in Member States have, thus far, shown little interest in enforcing the Directive against US companies.\(^\text{349}\) As a result, many transfers occur extra-legally without obstacles and US government authorities are not actively pressured to confront the Directive’s Article 25 transfer restrictions.\(^\text{350}\) Furthermore, financial institutions have three options under which they may legally transfer data on EU citizens to the US. Data controllers may make transfers pursuant to the Article 26 derogations, for example where the institution obtains the consent of the data subject or where the transfer is necessary for the performance of a contract between the data subject and the controller. Transfers may also occur pursuant to one of three sets of approved Standard Contractual Clauses, or pursuant to individual contracts that are pre-approved by a national Data Protection Authority. It is likely that the majority of legal transfers occur pursuant to Article 26 derogations because the use of

\(^{345}\) Id.


\(^{347}\) Email from Rosa Barcelo to author (Mar. 2, 2005). *See supra* note 190 (on file with author).

\(^{348}\) Email from Crispin Waymouth, Delegation of the European Commission, to author (Mar. 2, 2005) (on file with author).

\(^{349}\) Email from Leonardo Cervera Navas, formerly of the Data Protection Unit of the European Commission, to author (Apr. 21, 2005) (on file with author).

\(^{350}\) This issue was a priority for US authorities under the Clinton Administration when the Directive first entered into force and some American companies feared that national DPAs would block data transfers. These fears gave rise to the discussions that resulted in the Safe Harbor Agreement of 2000.
standard contractual clauses or ad hoc contracts approved by the national DPAs is still very rare.\textsuperscript{351} Most financial institutions are not eligible to join the EU-US Safe Harbor\textsuperscript{352} because they are not subject to the jurisdiction of the FTC or the Department of Transportation (DOT).

The Commission has recognized that the national laws concerning international data transfers may not be adequately enforced and that a large number of transfers may be occurring in violation of the Directive.\textsuperscript{353} Indicators suggest that "many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection."\textsuperscript{354} One of these indicators is the very limited number of notifications received from Member States pursuant to Article 26(2) of the Directive: "this number is derisory by comparison with what might reasonably be expected."\textsuperscript{355} While EU officials may currently be reluctant to disrupt trans-Atlantic data flows, the First Commission Report on the Implementation of the Directive and the Working Party’s recent Enforcement paper\textsuperscript{356} are likely to generate a response by the national DPAs. If DPAs begin to monitor international data transfers more carefully, they may very well begin to use their existing powers to enforce the Directive’s provisions against financial institutions. Penalties vary from one Member State to another, and they can include not only economic but also criminal sanctions.\textsuperscript{357} The fact that the recently published reports highlight the Article 25 enforcement problems suggests that the EU may not be willing to continue its policy of lax enforcement that permits a de facto solution to the privacy issue in the face of the formal contradiction.

Given the high level of trans-Atlantic data flows, if Article 25 of the Directive is enforced, the United States and the European Union must reach some formal agreement that will promote certainty in the legality of data transfers between them. The current options for legal transfers are problematic; they tend to be unrealistic or inefficient. Both European and American financial institutions would gain tremendously from a sectoral adequacy determination for the financial services sector.\textsuperscript{358} EU officials have stated that they would like to provide for more flexible arrangements for transborder flows, especially out of

\textsuperscript{351} Email from Leonardo Cervera Navas, supra note 348.
\textsuperscript{354} Id.
\textsuperscript{355} Id.
\textsuperscript{356} See, e.g., Declaration of the Article 29 Working Party on Enforcement, supra note 317.
\textsuperscript{357} Barcelo, supra note 331, at 988.
\textsuperscript{358} In the absence of such a determination, the financial services sector could become eligible for inclusion in the Safe Harbor or seek to enhance the use of model contracts and streamline the process of approval of individual contracts in order to facilitate the process of data transfer. However, for reasons discussed infra, neither of these options is ideal.
the EU, and there have been indications that the EU would accept the adequacy of a GLBA modified to include the basic Safe Harbor principles. In 1998, American law professors Swire and Litan suggested that the detailed provisions of the FCRA alone may provide adequate protection for credit information, even if transfers for the other sectors were prohibited, and consumer credit regulation has been described as the sector providing the closest degree of functional similarity to European data protection principles. However, the EU has never actually found that the privacy regulations applicable to a discrete sector of a foreign nation's economy constitute adequate protection. However, in the Safe Harbor adequacy decision, the EU determined that the policies of individual companies, rather than the laws of the US or of a particular sector, provided adequate protection.

The language of Article 25 of the Directive establishes that an adequacy consideration may take into account both the general and sectoral laws in force in the non-Member State, as well as the "professional rules and security measures" complied with in that State. For the Commission to make a binding determination that protection is "adequate," several key distinctions between the functional protections offered in the two regimes should be reconciled, and the functional similarities should be clarified and emphasized. Part IV described in detail the divergent areas of the current US and EU data protection regimes. This Part describes the nature of the EU's restriction on transfers, including the extent to which divergence from the terms of the Directive has been permitted. Finally, this section will then consider changes to US regulation that would strengthen the argument that the financial services sector should qualify for an adequacy determination. First, the standards the EU has accepted in the US-EU Safe Harbor, the model contracts, and other adequacy determinations for third countries indicate potentially acceptable alternatives to the Directive's formal data protection principles. Second, given the EU's increased recognition of codes of conduct and corporate rules, as well as the language of Article 25, the EU is in a position to evaluate US self-regulatory practices in making a decision for the sector. Finally, there are several key ways that the US can improve its laws to "bridge the gap" and satisfy the EU that financial services regulation in the US affords an "adequate" level of protection. This ultimate determination must take into account compromises the EU has made with respect to other privacy protection regimes, as well as ideological differences in approaches to privacy and to law in the two jurisdictions.

360. Tallman, supra note 13, at 779.
361. SWIRE & LITAN, supra note 33, at 32.
362. SCHWARTZ & REIDENBERG, supra note 3, at 289.
A. Transfers Currently Permitted by the European Union

EU Member States have different standards for permitting transfers under the exemptions of Article 26. Currently, the European Commission and individual DPAs may determine that a third country provides adequate protection or that a particular transaction provides adequate safeguards. Some Member States also allow data controllers themselves, with limited oversight by the national supervisory authorities, to make adequacy determinations for third countries. As the Commission states, an overly lax attitude in some Member States risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the "least burdensome" point of export. On the other hand, an overly strict approach risks being unrealistic and creating a gap between law and practice, which is damaging for the credibility of the Directive and for Community Law in general.

1. Article 26 Derogations

The two most important Article 26 derogations are transfers that occur with the data subject’s "unambiguous consent" and transfers that are "necessary for the performance of a contract" between the data subject and the controller or concluded in the interest of the data subject between the controller and a third party. To be valid, data subject consent must be fully informed; many states use an opt-in standard for international transfers. After the data subject consents, the US importer is not required to afford access, choice, or any other right that the data subject may have had under the legal framework in the EU country of residence. There are substantial practical difficulties in obtaining full and informed consent, and it can usually be revoked. Customers may be reluctant to opt in if they are informed, as required, that the data will be transferred to a place without "adequate protection." The language "necessary for the performance of a contract" has also been interpreted narrowly. Most DPAs allow data to be transferred pursuant to this derogation

364. Barcelo, supra note 331, at 988-89. For examples, see the U.K.'s Data Protection Act of 1998, available at http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm, and the Dutch Personal Data Protection Act of July 6, 2000, available at http://home.planet.nl/~privacy1/wbp_en_rev.htm. However, if the DPA finds that the importer's country's privacy laws fail to pass the adequacy requirement, the exporting company may be likely to be charged with violation of U.K. or Dutch privacy laws for illegal transfer of data to a country that does not provide adequate protection if the transfer does not fit within an exception. The company may be liable for heavy fines, not to mention the effects of any resulting bad publicity. Barcelo, supra note 331, at 989.

366. Id.
368. Barcelo, supra note 331, at 993-94.
369. Id. at 995.
370. Id. at 1000.
only if the transfer is "absolutely essential" for the performance of the contract. 371

As a result, consent and necessity are not adequate to support all financial services transfers from the European Union to the United States. Transfers not covered by these derogations include certain payment transactions where credit card processing occurs in the United States; sales of financial services to individuals and businesses located in the EU; investment banking practices, such as market analysis, hostile takeovers, due diligence, private placements, and other sales to Europeans; mandatory securities and accounting disclosures in the US; and the transfer of individual and corporate credit histories out of Europe. 372

2. Model Contracts

Data transfers that do not meet one of these derogations may be permitted pursuant to a contract approved by the European Commission or a national DPA. To date, the Commission has approved three sets of standard contractual clauses that contain legally enforceable declarations whereby both the "Data Exporter" and the "Data Importer" agree to process the data in accordance with basic data protection rules and to allow individuals to enforce their rights under the contract. The first set of model contract clauses, from June 2001, 373 covers transfers to controllers in third countries. The second set, from December 2001, 374 provides for less stringent safeguards for contracts between controllers and processors to perform data processing operations abroad. The third set of clauses, 375 available for use as of April 1, 2005, concerns transfers to controllers abroad.

The standard contractual clauses impose certain obligations on U.S. importers in addition to the obligations imposed by US data protection law. Under the terms of the June 2001 contract for transfers to data controllers, the data importer and exporter would agree to be bound by "Data Protection Principles" similar to those of the Directive. 376 They provide for an opt-out system for direct marketing and onward transfer and an opt-in system for sensitive data. The rights of access, rectification, and erasure appear to be absolute, and the subject retains a right to object to decisions made on the basis

371. Id. at 1000.
376. Decision 2001/497/EC, supra note 373, app. 2.
of fully automated processing. Special security measures must be in place for sensitive data, and the required purpose limitation, data quality and proportionality, transparency, and security measures are similar to those found in the Directive. Onward transfer may occur only where the data importer has either obtained the informed consent of the data subject (opt-out or opt-in for sensitive data) or where the third party becomes a party to the contract.377

The most recent (2004) standard clauses for transfers to data controllers do not include "Data Protection Principles;" rather, the data importer agrees to process personal data only on behalf of the importer and pursuant to his instructions and the clauses,378 and to take certain security measures specified in the contract. The data importer agrees to return or destroy all of the personal data transferred, to stop processing at the termination of the provision of the processing services,379 and to submit its data processing facilities to audits at the request of the data exporter.

In both sets of clauses, the parties must specify the purposes for which the transfer occurs and the data processing activities they anticipate. They must agree that the data transferred will be used only to accomplish the specific purpose of the transfer.380 Furthermore, the contracts contain a third-party beneficiary clause allowing a data subject who has suffered damages to file lawsuits against both the exporter and the importer in the courts of the data subject's own country or those of the data exporter and to pursue mediation or arbitration. Finally, the parties must either accept joint liability for damages or, in the most recent clauses, the importer must indemnify the exporter for damages. In addition, these 2004 clauses provide for a more pragmatic approach to the substantive obligations imposed on the data importer and on their relationships with the national DPAs. However, the importer is still subject to an EU Member State's governing law, and it may be required to submit to audit by the supervisory authority.381 Therefore, the new clauses, although an improvement for US data importers, may not assuage concerns with respect to business confidentiality and the subjection of US data importers to litigation abroad.382 Commentators and businesses stated prior to the adoption of the most recent set of clauses that the Model Contracts are "unlikely to be acceptable to most firms."383 It is unclear whether the new contract clauses will change that view.

While the model contracts may not be acceptable to data importers, individual contracts may be prohibitively costly. Tailored model contracts may be accepted by a DPA of one state and not by another.384 Thus, an importer

377. Id. app. 3.
379. Id. annex, cl. 11.
381. Id. annex, cls. 8, 9.
382. Tallman, supra note 13, at 770-71.
383. Id. at 749.
384. Citigroup's Review of the Directive, supra note 118. See also Barcelo, supra note 331,
may have to implement and comply with up to 25 different individual contracts. Indeed, the importer would have to track the data received from the EU Member States by country of origin in order to comply with the individual requirements of each Member State.

3. Safe Harbor

When the Data Protection Directive came into effect in 1998, US businesses were concerned that enforcement of Article 25 would disrupt data flows and commerce between the US and the EU on a large scale. In response to these concerns, in March 1998, the US Department of Commerce and the European Commission Directorate for Internal Markets initiated a high-level, informal dialogue to negotiate an agreement that would ensure the continued free flow of personal data across the Atlantic. Consistent with US market theory that companies will choose to provide privacy if consumers demand it, the idea was to create a "safe harbor" standard for privacy that would be accepted by the EU as "adequate" and with which companies could comply voluntarily.

In 2000, the European Commission approved the Safe Harbor (SH) for US companies under the jurisdiction of the DOT and the FTC. The SH framework is set forth in a set of seven privacy principles and fifteen FAQs. Companies that voluntarily declare their adherence to these principles are not required to obtain approval by national DPAs. They agree to submit to enforcement by the FTC or the DOT in order to ensure compliance with these principles. As a result, financial institutions are generally not eligible to join. To date, 880 companies have joined.

The SH principles require the importing company to provide notice to data subjects about the collection of data. First, the notice must be in clear and conspicuous language and must define the specific purposes of collection and the controller’s intended transfers. Second, the principles require that the controller offer an opt-out mechanism for data subjects to exercise the choice of whether or not to prevent disclosure of their personal data to third parties. Data subjects may also prevent the use of their data for purposes other than those for which it was initially collected or subsequently authorized, which could prevent use by affiliates if not initially disclosed. The SH’s principle of data integrity is similar to that contained in the Directive; the data importer may use information for purposes other than those specified, provided that they are “not

---

385. WELLBERY, supra note 17.
387. Decision 2000/520/EC, supra note 352.
388. The number of companies subscribing to the Safe Harbor principles has generally been lower than anticipated by the European Commission, suggesting that it is not an ideal framework for many companies. See infra note 394, at 5. For the companies participating, see http://web.ita.doc.gov/safeharbor/shlist.nsf (last visited Feb. 23, 2006).
incompatible" with the purpose for which the data was originally collected. Controllers must take reasonable security precautions to protect data from loss, misuse and unauthorized use, and they must ensure that individuals have access on a "reasonable basis" to all information that might be held about them. This obligation to provide the data subject with access to personal data is subject to the principle of proportionality, as under the Directive. However, a company may refuse to grant the subject the right of access if, for example, the cost is disproportionate. For sensitive information, data subjects must be given an affirmative or explicit (opt-in) choice if the information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected or subsequently authorized. For onward transfer of information to a third party, the company must apply the notice and choice principles.

The SH's core principle of enforcement includes three elements. First, there must be readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles, and damages must be awarded where the applicable law or private sector initiatives so provide. Second, the SH requires follow-up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented. Finally, the SH imposes obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence and the consequences of such adherence. Failure to abide by the Principles after having been certified must be actionable as an "unfair or deceptive act," and sanctions must be "sufficiently rigorous to ensure compliance." Data Protection Authorities in the EU may refer cases of non-compliance to the FTC, which must seek injunctive relief or damages to provide redress to individuals on a priority basis. Thus, the enforcement arrangement appears to be a carefully constructed system of self regulation, reinforced by the FTC's authority to police unfair and deceptive acts. While the federal financial regulators do have authority to assert that a violation of a financial firm's policy constitutes an unfair or deceptive act under Section 5 of the FTCA, they have not indicated that they would accept jurisdiction under the SH. The financial services sector was not initially included in the SH in large part because the EU was concerned about enforcement in the absence of FTC jurisdiction.

390. However, the opt-in requirement for sensitive data is subject to certain exceptions involving necessity, the data subject's interest, or where the data has already been made public by the individual. Safe Harbor FAQ 1, supra note 393.
392. WELLBERY, supra note 17.
393. Tallman, supra note 13, at 763. US firms were also concerned about losing negotiating leverage for their position in the debate over the GLBA privacy provisions, which were pending.
Finally, it is not clear that financial services joining the SH would be an effective long-term solution to the data protection issue, given the EU’s recent determination that the implementation of the SH is deficient in many respects. The review of the effectiveness of SH implementation indicated that, while participating US organizations have made efforts to accommodate privacy concerns, “important improvements are required” to ensure that safeguards for personal data transferred under the SH are adequate. Most of the reviewed US organizations had trouble correctly translating the SH Principles into their existing data-processing policies. The study concluded that the deficiencies and laxity in the US implementation of the SH indicate that the SH regime favors US companies over EU companies. The absence of enforcement actions, despite the easily documented shortcomings of organizational policies and practices, suggested that US companies actually operate under a less stringent data protection standard; indeed, they were seen as processing data in ways contrary to the SH Principles without real risk of sanction. However, if SH Principles are strictly applied, the Commission noted that there may be discrimination against US companies because such application may be more exacting than national laws transposing the EC Directive. As a result of the study, the Commission invited DPAs to suspend data flows to the US that are occurring pursuant to the SH if the DPA believes that there is a substantial likelihood that SH principles are being violated.

In sum, the SH and the Model Contracts follow the Directive’s principles fairly rigorously. However, in lieu of EU enforcement by DPAs and a private, individual right of action, the SH adopts a US, agency-based enforcement mechanism, guaranteeing an individual right to damages only where “applicable law and private sector initiatives so provide.” The FTC is ultimately responsible for enforcement. Both models insist on purpose specification, although under


396. Specifically, transparency and comprehensibility of notices or privacy policies were often deficient; relatively few organizations published privacy policies that reflect all seven Safe Harbor Principles, see supra note 394, at 8; choice was not clearly mentioned or was lacking entirely; with respect to onward transfers, the status of mentioned “third parties” was not always clear; certain companies did not represent that they had adopted security measures; regarding data integrity, the relevance of the data for the intended use was difficult to determine, since either the “purpose”, the “data type” or the “activities” conducted were not specified at all or not clearly formulated; and principle of access tended to be weakly implemented. *Safe Harbour Decision Implementation Study*, supra note 399, at 105.

397. Id. at 112.

398. Id.

the SH, companies may engage in processing that is "not incompatible" with the specified purposes. The Directive's principles regarding special treatment for sensitive data, reasonable access, and an opt-out choice for onward transfer are generally retained in their original form under both arrangements.

B. European Perspectives on Self Regulation

Self regulation, a cornerstone of US economic policy, may raise problems for EU law enforcers in considering adequacy of protection because it does not provide formal legal rights of redress. The EU's difficulties in accepting self-regulatory measures stem from the arguments that privacy protection standards may be set in an unaccountable manner by businesses alone, thus avoiding inconvenient but vital protections. Europeans also claim that self-regulatory measures may be unevenly adopted, and they may be used to avoid government regulation.\footnote{400} However, if self regulation fails to provide adequate protection in the absence of a legislative baseline, it may, in conjunction with such a baseline, play a critical role within a comprehensive privacy regime.\footnote{401} The Directive itself states that "professional rules and security measures which are complied with" may provide a basis for an adequacy determination.

The Working Party has defined a "self-regulatory code" as "any set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned."\footnote{402} As with general evaluations of enforceability, the WP determines the validity of a self-regulatory code based on whether it achieves a good level of compliance, provides support and help to individual data subjects, and includes a mechanism for the individual to obtain appropriate redress. The evaluation must take into account, among other things, the degree to which rules can be enforced, whether the body responsible for drafting the code is representative of the sector, the transparency of the code, and whether the code prohibits disclosure of data to companies not governed by the code without adequate safeguards.\footnote{403}

Despite the omnibus character of the Directive, the EU recognizes that privacy considerations may vary across sectors and that "codes of conduct" for certain sectors may contribute to the proper execution of national data protection laws.\footnote{404} The Working Party has recognized that the adoption of codes of conduct by corporate groups is relatively frequent. Such codes may refer to proper maintenance and retention of accurate books and records, truthfulness and accuracy in communications with the public, and protection of confidential

US entities with a presence in Europe, including some of the large bank holding companies, have drafted guidelines and codes of conduct to meet the European standard, seeking to satisfy the data protection standard through separate negotiations. Furthermore, the WP has recently stated that certain “binding corporate rules” may apply to third-country transfers to make them legitimate under Article 26(2). These rules would permit companies to use binding or legally enforceable corporate rules similar to self-regulatory measures as a basis for an international transfer under Article 26(2). The evaluation of the “binding nature” of such corporate rules requires both an “assessment of their binding nature in law (legal enforceability), and of their binding nature in practice (compliance).” Although the ability of data subjects to enforce the rules in court is a necessary element, the WP appears to attach more importance to the fact that the rules are complied with in practice, as is the aim of any self-regulatory approach. The problem, therefore, is in determining empirically whether the rules are complied with in practice.

In order to transfer personal data to a third country on the basis of compliance with “binding corporate rules,” the corporate entity must notify the data subject of the purposes of the transfer, the identity of the data exporter, the categories of the further recipients of the personal data, and the countries of destination. The institution must explain to the data subject that, after the transfer, data may be processed by a controller who is not bound by the corporate rules and who is established in a country that has not been found to provide an adequate level of protection. Data subjects covered by the binding corporate rules must become third-party beneficiaries of the rules, for example through contractual arrangements between the members of the corporate group. As such, data subjects may enforce corporate compliance with the rules by lodging a complaint before the competent DPA or before the competent court on Community territory.

Multinational companies with complex global architectural structures are expected to benefit most from such codes of conduct for international transfers. The WP has also advocated combining standard contractual clauses and binding corporate rules to allow onward transfers to other recipients without further contracts.

Overall, EU recognition of self-regulatory codes seems to be increasing, and the EU’s recent attitudes toward codes of conduct and binding rules may

406. Murphy, CRS Report for Congress, supra note 270.
408. Id.
409. Id.
410. Id.
411. Id.
412. Id.
413. Id.
provide a framework in which to evaluate the US regulatory structure in terms of functional standards rather than specific legislation.

C. Recommendations for Amending the US Privacy Regulatory Structure

As described in Part V, even when the US regulatory structure is viewed in its entirety, discrepancies remain between US and EU data protection regulation. These differences stem primarily from two distinct philosophical underpinnings of the right to information privacy, as well as from differing conceptions of the role of law in ensuring individual protections. However, while these divergent perspectives may be irreconcilable, the substantive standards in both privacy regimes are actually somewhat similar, perhaps because both sets of rules are derived in part from the OECD guidelines. Therefore, despite different conceptual frameworks, the actual privacy regulation of financial institutions in each legal system may in fact provide similar protections to consumers. This paper argues that the achievement and recognition of “functional equivalence” would permit transfers to occur between the EU and the US without compromising the level of personal data privacy afforded to any individual.

The most significant differences between the EU and the US data protection regulatory schemes concern the requirements imposed on financial institutions with respect to the following protections: data subject rights of access, data subject choice with respect to further processing and onward transfer, special treatment of sensitive information, and enforcement. The discrepancies in these areas of regulation could be remedied through specific federal privacy legislation while avoiding both omnibus privacy legislation and regulatory requirements that industry perceives as overly burdensome. Because the actual privacy practices of financial institutions in the EU may be less stringent than those formally required by the Directive, the United States should be required to abide by the rules actually enforced in the EU. Nevertheless, some new legislation is required for the United States to attain the functional level of data protection that currently exists in the EU.

First, the US regulatory scheme currently ensures that data subjects have access to personal information under the FCRA, under the Fair Credit Billing Act, and in the ordinary course of business. In its own Member States and in the Safe Harbor agreement, the EU has accepted a level of access rights that only requires the data controller to provide access where doing so is not overly burdensome. If the United States were to formalize the access that most financial institutions already provide, it could comply with this requirement without a major industry change.

Second, in order to comply with the EU’s “purpose specification” requirement, the United States should require institutions to describe the purposes of collection at the time they provide the opt-out notice. This opt-out system is permitted by the SH. While institutions may have to provide further notice for uses that are “incompatible” with the original purpose of collection, “compatibility” may be interpreted fairly broadly.
With respect to onward transfers pursuant to “joint marketing agreements,” US regulators have already set out guidelines requiring that service contracts with third parties include a clause restricting further use or transfer, and ensuring that the data is processed securely. Formalization of these guidelines would render the provision very similar to the EU’s provision for processors. With respect to onward transfers for marketing purposes, the FACTA allows customers to opt-out of marketing uses of any shared information. EU data controllers have two options for marketing data, either providing explicit notice to the customer or providing general notice to the public. It is likely that the FCRA standard would meet the first of these.

A difficult issue, and one that should be examined more closely, is the question of whether notice and an ability to opt out must be required for affiliate sharing. As noted, differences in financial structures in the United States and the European Union may reduce the discrepancy, but there are still certain situations in which information may be shared freely in the United States where it could not be shared in the EU. One possible solution would be for the United States to create special notice requirements for those affiliates that are in a line of business that the customer would not reasonably expect to be affiliated with the original institution.

Next, the SH and Model Contracts indicate that a key component of the EU regulation is that special treatment be accorded to sensitive data. In the United States, only sensitive credit information receives such treatment. However, collecting data on racial or ethnic origins, political or religious beliefs, and health and sex life is generally not integral to financial services practices, and it is possible that special treatment could be adopted for the institutions that do collect such data without overburdening the industry. Currently, such information may not be used for marketing solicitations without providing an opt-out notice under the FACTA. In addition, under the FACTA’s Title IV, medical information receives special treatment and can only be shared under limited circumstances. Furthermore, financial institutions are not permitted to use sensitive information in decision making where such use would constitute discrimination under the Equal Credit Opportunity Act. The SH standard for sensitive information would require consumers to opt in to transfers the purposes of which were not initially disclosed.

Finally, with respect to enforcement, it may be difficult for the EU to

---

415. In 2003, Senators Feinstein and Boxer proposed an amendment to the FCRA that would give consumers the right to opt out of companies’ sharing their information with affiliates in different lines of business. The amendment, although geared toward consumers, potentially would have exempted huge businesses, like Citigroup, Inc. and Bank of America Corp., which pool the information in a common database that their affiliates can access. Michele Heller, Loophole for Big Banks Seen In Amendment to FCRA Bill; Fair Credit Reporting Act reauthorization legislation, AM. BANKER, Oct. 30, 2003.
accept a system that fails to provide for a specific federal private right of action and that does not have a single oversight body responsible for ensuring that privacy protections do not "fall through the cracks." However, the EU has accepted FTC enforcement for companies in the SH. Provided there are sufficient guarantees of adequate enforcement measures, including indices of high levels of enforcement by US agencies, as well as redress for individuals at the state level, the EU might be willing to accept the federal agencies as enforcement bodies. The EU has demonstrated that it is willing to recognize the importance and effectiveness of sectoral codes of conduct and other self-regulatory measures, such as binding corporate rules, which may be considered in the adequacy determination.

The United States must establish strong enforcement practices against institutions that breach their stated codes of conduct or policies. The federal banking agencies may already enforce Section 5 of the FTCA, which prohibits unfair and deceptive acts. In addition, US regulatory enforcement agencies should collect more statistical data on privacy enforcement against financial institutions as well as on their actual levels of compliance in order to be able to indicate to the EU the level of compliance that is actually observed through the mix of federal, state, and self regulation. Finally, the US argument for a sectoral determination would be greatly strengthened by the creation of a federal oversight body, such as an Office of Electronic Commerce and Privacy Policy (OECPP), which would make and coordinate policy with respect to privacy and electronic commerce without being a regulatory or enforcement agency. The General Accounting Office has called for greater harmonization and cooperation between regulators, and this may be an important step toward achieving a clearer and more unified data protection policy in the United States.

VI. CONCLUSION: TOWARD AN ADEQUACY DETERMINATION FOR FINANCIAL SERVICES

Short of an adequacy determination for the entire United States, the probability of which may be slim, an EU determination that the financial services sector provides "adequate protection" for personal data is the most effective means of facilitating financial services data transfers between the United States and the European Union. Such a decision would eliminate the risk that the EU will enforce the provisions of its Data Protection Directive against US financial institutions and would thus provide for greater certainty in transactions. Currently, EU Member States informally permit many trans-Atlantic transfers to occur in violation of their national data protection laws, but

417. See SWIRE & LITAN, supra note 33, at 179 (proposing a similar body). In 1999, the Clinton Administration created a similar office, the Chief Counselor for Privacy, based in the Office of Management and Budget.

there is evidence that Data Protection Authorities in EU Member States may begin to enforce data protection restrictions more actively. In 2003, the First Report on the Implementation of the Directive\(^\text{419}\) emphasized the number of international transfers that seem to be occurring illegally, and the Commission called for more stringent enforcement efforts. Even more recently, in November of 2004, the Working Party issued a report indicating that enforcement would be one of its top priorities.\(^\text{420}\) Furthermore, the European Commission’s Report on the protection provided by the Implementation of the Safe Harbor Principles\(^\text{421}\) revealed that the Safe Harbor has not effectively provided adequate protection, and the Commission invited DPAs to stop transfers occurring under that exemption.

If Article 25 of the Directive is actively enforced, making transfers using one of the currently available options would be excessively costly for data transferors. Using an Article 26 derogation would require explicit consent of the data subject or absolute necessity of transfer, both of which may be unlikely. The other options are to use an unfavorable Model Contract, which may subject the US importer to litigation in the EU, or to obtain costly contractual approval on a case-by-case basis by one or more DPAs. While some large corporations have attempted to obtain approval through the use of “binding corporate rules,” such approval is relatively informal and presumably subject to challenge by the Commission.

Considering the real risk of increased enforcement and the limited, costly alternatives that are currently available to transfer data legally, the costs of amending US legislation to provide a level of protection considered “adequate” by the EU are relatively low. As illustrated in this paper, several minimal alterations to the law in strategic places, as well as the collection of empirical compliance evidence to further legitimize US self-regulatory measures, could result in the United States providing protections that are functionally equivalent to those provided to EU citizens. For financial institutions, the compliance costs would presumably be similar to those they would incur by joining the Safe Harbor or using a Model Contract, which would probably be required anyway under current law if the EU begins enforcing its Directive. Furthermore, there is evidence that US financial institutions may have to increase their privacy standards independent of what the EU does due to increasing consumer demands and the threat of more stringent state regulation. This threat has become far more pressing in light of the recent preemption decisions.\(^\text{422}\)

The EU has indicated a willingness to engage in further discussions on data protection. The United States should take the opportunity now to begin negotiations, before the real risks of enforcement are so high and the stakes for the industry are so great that the EU can exert even stronger pressure on US

\(^\text{419. Supra note 108.}\)
\(^\text{420. Supra note 317. See also Strategy Document of September 2004, supra note 319.}\)
\(^\text{421. Safe Harbour Decision Implementation Study, supra note 4.}\)
\(^\text{422. See, e.g., Am. Bankers Ass’n, supra note 269.}\)
officials to come to an agreement. While the EU has not yet made a sectoral
determination, its current enhanced recognition of the validity of corporate and
financial self-regulatory codes makes this an opportune moment to bring such a
proposal to the Commission's attention. The United States should offer the
GLBA and the recently amended FCRA, in conjunction with federal regulations,
state law, self-regulation, and industry standards, as a complete sectoral package
for the EU to consider for approval.