Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive

Morey Elizabeth Barnes

Follow this and additional works at: http://scholarlycommons.law.northwestern.edu/njilb

Part of the Consumer Protection Law Commons, and the International Law Commons

Recommended Citation

Falling Short of the Mark: The United States Response to the European Union’s Data Privacy Directive

Morey Elizabeth Barnes*

I. INTRODUCTION

In the spring and summer of 2005, the headlines of America’s major newspapers provided a constant reminder of an issue about which Americans have grown increasingly worried: data security. Rather than publicizing the war in Iraq or the buzz over potential Supreme Court nominees, these headlines warned: “Info theft slams chain: 1.4 million card numbers stolen;”1 “Poll Says Identity Theft Concerns Rose After High-Profile Breaches;”2 “Data Security Breaches Alarm Consumers.”3 In the previous few months, a series of high-profile companies such as Bank of America, Reed Elsevier Group’s LexisNexis, PayMaxx, Choice Point, and SAIC had announced that millions of records containing consumers’ personal data in their custody had been lost or stolen, putting these individuals at risk for identity theft and similar injuries.4 Responding to

---

* J.D. Candidate, 2007, Northwestern University School of Law. Thank you to my mother, Professor Sarah Jane Hughes of the Indiana University School of Law—Bloomington, for her editorial assistance with this comment.

Author’s Note: This comment addresses only legislative proposals made during the first session of the 109th Congress, and discussion is limited to a handful that could impact the operation of the U.S.-E.U. Safe Harbor. This comment is not intended to analyze all legislative proposals that would impact consumer privacy. For instance, it does not consider transfers of passenger data, which the United States and European Union addressed in a decision issued in October 2006. Discussion of the legislative proposals is current as of July 31, 2006.

1 Bill Husted & David Markiewicz, Info Theft Slams Chain: 1.4 Million Card Numbers Stolen, ATLANTA J.-CONSTITUTION, Apr. 20, 2005, at 1A.
4 Declan McCullagh, LexisNexis Flap Draws Outcry from Congress, CNET News.com,
rising consumer alarm, Senator Patrick Leahy of Vermont, whose own data had been misplaced by Bank of America, and Senator Arlen Specter of Pennsylvania responded with The Personal Data Privacy and Security Act of 2005 ("2005 Privacy Act"). The bill proposed a series of new requirements for corporations’ handling of personal data, new penalties for data theft, and new provisions to notify individuals whose personal data was compromised.

Senator Leahy’s statement that the proposed reforms were “long overdue,” particularly when considered in the context of contemporary news coverage, might have suggested that no previous legislation had addressed data privacy in the United States. That was far from being the case. Although the 2005 Privacy Act is Congress’ most serious response to the issue thus far, it is only the latest in a series of legislative attempts over the course of the past four decades to address personal data privacy and security.

During the past four decades, the United States has had a relatively consistent approach to the issue, based on sector-specific legislation and self-regulation by U.S. industries. Until the late 1990s, that approach proved satisfactory—at least for the conduct of international business. But when the European Union introduced sweeping privacy legislation, upsetting the international status quo on the treatment of personal data, it became clear that the U.S. approach might create serious obstacles for U.S. companies engaged in international transactions.

Subsequent legislative and regulatory efforts have resolved these problems in part. In the industries that stand to suffer most from the potential loss of international business, however—particularly the financial services industry—those efforts have not fully solved the problem of data privacy in the domestic and international markets.


7 Id.

8 Id.

9 See Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 IND. L. REV. 174, 223 (1999) (noting that “the United States has historically depended heavily on private industry, private property, and individual self-reliance”; although that “focus on individual and collective private action inevitably restrains the power of the government to pass sweeping privacy laws . . . . it also facilitates considerable privacy protection through the use of technologies, markets, industry self-regulation and competitive behavior, and individual judgment.”).
To provide a foundation for understanding the current state of data protection requirements for international business, particularly the conflict between the U.S. and European approaches (which dominate global business), Part II of this comment presents a brief history of United States and international privacy regulation, and then discusses the current regulatory frameworks in the United States and European Union. It also explores how U.S.-E.U. cooperation on the Safe Harbor framework has impacted the U.S. approach to privacy regulation. Part III outlines proposed changes to the current U.S. regulatory regime. Finally, Part IV argues that those proposed changes fail to address the problems that prompted renewed attention to the issue of data privacy and security. The continuing disparity between the U.S. and E.U. regulatory regimes may significantly impact the U.S. role as a global business leader. The United States will have to decide whether its traditional sectoral, self-regulatory approach can ensure the continued prosperity of its industries that depend on international transactions. This comment concludes with a brief exploration of alternatives to new legislation, which might protect both consumers and the economic interests of U.S. companies while preserving the traditional U.S. regulatory scheme.

II. HISTORY AND CURRENT STATUS OF PRIVACY REGULATION IN THE UNITED STATES AND THE EUROPEAN UNION

A. History of International Privacy Legislation

Concern over the privacy and security of consumer data first arose in the 1960s and 1970s.\(^{10}\) The emergence of new information technologies in the early 1990s introduced new possibilities for the loss and abuse of such information.\(^{11}\) These new technologies enhanced the prospects that large national data banks would be created giving governments and corporations carte blanche access to personal data, thus creating a new concern beyond the accuracy of information in certain data banks to more invasive uses of personal data.\(^{12}\)

Countries began to propose legislative solutions to the carte blanche access concern in the 1970s. The German state of Hesse promulgated the

---

\(^{10}\) See 15 U.S.C. § 1681 (2000) (noting that because "[c]onsumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers," Congress felt "the need to insure that [those] agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.").

\(^{11}\) Jeffrey B. Ritter et al., Emerging Trends in International Privacy Law, 15 EMORY INT'L L. REV. 87, 90 (Spring 2001).

first data privacy law in 1970; over the following decade, Sweden, Germany, and France followed with national laws.\(^\text{13}\) The United States was also part of the vanguard group on government access in that decade, as Congress passed the Fair Credit Reporting Act ("FCRA"), the Privacy Act of 1974 and the Freedom of Information Act.\(^\text{14}\) (Subsequent U.S. legislative efforts to address consumer privacy, on a sector-by-sector basis, will be discussed later in this comment.)

In the 1980s, realizing the need for harmonization of international privacy legislation, intergovernmental organizations began to propose blanket guidelines that provided minimum standards for their member nations' data privacy regulatory schemes. The Organization for Economic Cooperation and Development ("OECD") introduced Guidelines ("OECD Guidelines") in 1980 that represented the first major international attempt to address privacy concerns.\(^\text{15}\) Similarly, in 1985, the Council of Europe created its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("COE Convention"). Finally, in 1990 the United Nations' High Commissioner for Human Rights promulgated Guidelines for the Regulation of Computerized Personal Data ("U.N. Guidelines").\(^\text{16}\)

The OECD Guidelines, COE Convention, and U.N. Guidelines all recognized the need to secure data, particularly in international transactions, by providing a baseline level of protection.\(^\text{17}\) Each document embraced a set of "fair information principles" first announced in the OECD Guidelines.\(^\text{18}\) Those principles encompass eight basic tenets of consumer privacy: collection limitation, data quality, purpose, specification, use limitation, security safeguards, openness, individual participation, and accountability.\(^\text{19}\) That support of common principles theoretically facilitates international harmonization of privacy legislation.

Each set of guidelines reflects the idea, prevalent in the European Union Member States, that citizens have a fundamental right to privacy and protection of their personal information.\(^\text{20}\) More than two dozen countries

---

\(^\text{13}\) Ritter et al., \textit{supra} note 11, at 90–91.
\(^\text{16}\) \textit{Id.} at 18.
\(^\text{17}\) Assey & Eleftheriou, \textit{supra} note 12, at 149.
\(^\text{18}\) Gladstone, \textit{supra} note 15, at 18.
\(^\text{19}\) \textit{Id.} at 17.
\(^\text{20}\) Assey & Eleftheriou, \textit{supra} note 12, at 148 (noting that E.U. "governments recognize data privacy as a 'political right' anchored among the panoply of fundamental human rights
have adopted the COE Convention; many non-Member States have made the fair information principles the basis for their own national privacy legislation.\textsuperscript{21} However, all three documents are available to the organizations' respective members on a voluntary basis only. Because their implementation was not mandatory, and countries were given significant discretion in implementing these guidelines, they did not lead to the harmonization of data security regulations in the European Union and its trading partners.\textsuperscript{22}

B. The United States

In the two decades following the enactment of the FCRA, Privacy Act of 1974 and the Freedom of Information Act, the current U.S. framework for privacy regulation emerged. The United States employs a market-based, self-regulatory approach to protecting consumer data, based in part on the prevailing attitude that the privacy of personal data is an economic issue rather than a fundamental right. The FCRA, for example, prohibits creditors from disclosing customers' credit information to third parties unless that information concerns a particular transaction between that creditor and consumer, or the third party has one of certain "permissible purposes" for gaining access to the information.\textsuperscript{23} Thus, the FCRA emphasizes that privacy may be contingent upon the promotion of economic activity.

The Supreme Court's evolving treatment of personal privacy has never created an absolute right.\textsuperscript{24} Although Supreme Court case law has outlined an "expectation of privacy" stemming from the Fourth Amendment, that expectation is not preserved when an individual discloses data to a third party.\textsuperscript{25} For instance, under the Right to Financial Privacy Act,\textsuperscript{26} enacted in 1978, customers of a financial institution "have no rights to protection from government access of personal financial information obtained from a financial institution."\textsuperscript{27}

Consistent with that contingent view of consumer privacy, the U.S.

---

\textsuperscript{21} Ritter et al., \textit{supra} note 11, at 91–92.
\textsuperscript{22} Assey & Eleftheriou, \textit{supra} note 12, at 149.
\textsuperscript{24} For an extensive discussion of the Constitutional framework upon which privacy legislation in the United States has been based, see Cate, \textit{supra} note 9, at 196–209.
approach to data protection is relatively piecemeal,\(^{28}\) comprising sector-specific legislation and regulations promulgated by federal agencies including the Federal Trade Commission ("FTC"), federal bank regulatory agencies, the Federal Communications Commission, and the U.S. Department of Commerce’s National Telecommunications and Information Administration. Similarly, several of those same federal agencies share responsibility for overseeing the regulatory regime along sector-specific lines with the FTC possessing the largest number of actors in its jurisdiction and primary authority for enforcing the Safe Harbor over a broader group of actors. Congress has subsequently codified some of the provisions of regulations promulgated by the individual agencies, but the resulting framework is far from being comprehensive. For example, no federal laws affect commercial entities who hold their own transaction data banks or who maintain data for commercial clients as service providers to the originators of the information and are not "consumer reporting agencies" or "financial institutions" covered under the FCRA or the 2004 Fair and Accurate Credit Transactions Act amendments to the FCRA.\(^{29}\)

Public concern, particularly about new opportunities for privacy breaches presented by emerging technologies, led to the enactment of a series of privacy laws in the 1980s and 1990s. Each piece of legislation also reflected concerns about economic competition, true to the "free-market" approach to privacy regulation still followed by the United States.\(^{30}\) These laws reflect little concern that two or more industries might have common issues with the treatment of consumer data. The first regulations enacted by Congress primarily concerned the telecommunications industry: the 1984 Cable Act included provisions to protect the privacy of cable subscribers’ accounts and records, in 1986 the federal wiretap statute was revised to protect the privacy of information transmitted using emerging electronic and digital communication forms, and the 1991 Telephone Consumer Protection Act addressed privacy concerns “created by autodialers and junk faxes.”\(^{31}\) The advent of the Internet and increased use of electronic data storage prompted Congress to enact the FCRA, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Children’s Online Privacy Protection Act of 1998 (“COPPA”), and the Graham-Leach-Bliley Financial Services Modernization Act of 1999.\(^{32}\)


\(^{30}\) See Clear, supra note 25, at 1007.


\(^{32}\) Ritter et al., supra note 11, at 97–98; see also Cate, supra note 9, at 174.
Falling Short of the Mark

Prior to the 1995 introduction of the European Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("Data Privacy Directive"), which will be discussed at length in the next section, COPPA was perhaps the most stringent privacy legislation in the international arena. Its data provisions are similar to those of the Data Privacy Directive but apply only to minors using the Internet.\footnote{Kamaal Zaidi, Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data, 12 Mich. St. J. Int’l L. 169, 173 (2003).}

COPPA indicated a shift in the focus of privacy legislation in the United States, in response to both consumer concerns and the influence of the Data E.U.’s Data Privacy Directive. Beginning with the enactment of COPPA, more federal laws reflected, at least in part, the "fair information principles" and other globally accepted privacy provisions. For instance, the Online Personal Privacy Act of 2002 ("OPPA") draws a distinction between sensitive and non-sensitive data similar to that outlined in the Data Privacy Directive.\footnote{Id. at 188.} Unlike other U.S. measures, the OPPA also grants a private right of action "to American consumers who provide personal data to U.S. companies that fall short of providing ‘adequate’ privacy protection."\footnote{Id. at 187.} Similarly, the Consumer Privacy Protection Act of 2000 includes some of the Data Privacy Directive’s statutory language, including provisions on access.\footnote{Id. at 188.} Like the 2005 Privacy Act, however, none of Congress’ efforts in the past decade to address consumer privacy have equaled the Data Privacy Directive’s level of protection.

C. The European Union


\footnote{34 Id. at 188.}
\footnote{35 Id. at 187.}
\footnote{36 Id. at 188.}
\footnote{37 Assey & Eleftheriou, supra note 12, at 148 (noting that E.U. “governments recognize data privacy as a ‘political right’ anchored among the panoply of fundamental human rights and the rights attributed to ‘data subjects’ or citizens.”).}
\footnote{39 Clear, supra note 25, at 984.}
Convention in the 1980s. In a significant departure from those previous international guidelines, whose adoption by member nations was voluntary, the Data Privacy Directive provides E.U. Member States with mandatory baseline standards for domestic legislation protecting personal data. After the Data Privacy Directive’s formal promulgation in 1998, Member States had two years to enact legislation implementing it fully.

The Data Privacy Directive’s primary objectives are to “protect the fundamental rights and freedoms of natural persons, [particularly] their right to privacy with respect to the processing of personal data” and to facilitate the free flow of information through E.U. Member States, furthering the economic and social integration of the European Union.

Unlike the industry-specific approach to data privacy utilized by the United States, the Data Privacy Directive dictates the proper treatment of data to be based on “the nature of the data, not its use.” Preserving individuals’ right to control the use of their personal data, companies and organizations must get consumer consent to use that data—a feature known as “opt-in”—and must register in order to retain such data once they have acquired it.

In a series of thirty-four Articles, the Data Privacy Directive outlines Member States’ obligations to oversee the lawful processing of personal data, E.U. citizens’ rights of access and objection when their data is subject to such processing, and the imposition of liability and availability of judicial remedies in cases of improper data processing.

Of greatest concern to the United States (and the European Union’s other trading partners), the Data Privacy Directive imposes significant restrictions on the transmission of data to third countries. Article 25 of the Data Privacy Directive prohibits the transfer of personal data to non-member countries whose regulatory frameworks do not provide an “adequate level of protection” (as defined elsewhere in the Data Privacy Directive) for the privacy of domestic and/or shared consumer data. The provisions of the Data Privacy Directive apply to companies based outside the European Union, thereby preventing third parties from circumventing the Directive (and E.U. citizens’ right to the privacy of their personal data)

---

40 Ritter et al., supra note 11, at 94.
41 Clear, supra note 25, at 984.
44 Ritter et al., supra note 11, at 94.
46 Id.
47 Id.
48 Id. art. 25.
49 Id.
through the use of "data havens."\textsuperscript{50}

The Data Privacy Directive delegates broad responsibility for enforcement to Data Protection Authorities ("DPAs"), officials located within each of the E.U. Member States.\textsuperscript{51} DPAs possess the authority to cut off data flows from the European Union to any entity that violates the Data Privacy Directive's provisions and to enforce any applicable national privacy legislation, which may impose greater liability than the Directive itself.\textsuperscript{52} Furthermore, if a U.S. company violates provisions of the Data Privacy Directive, a DPA may notify U.S. state and federal enforcement agencies to have those entities take additional actions against the alleged offender.\textsuperscript{53} Enforcement is not limited to the DPAs; however, E.U. citizens possess a private right of action against violators of the Data Private Directive and corresponding Member States' privacy laws.\textsuperscript{54}

D. The U.S.-E.U. Safe Harbor

Many U.S. companies responded with alarm—and criticism—to the enactment of the Data Privacy Directive. Their opposition was two-fold: they objected to its disclosure requirements, under which individuals have the right to access all of their personal data, and insisted that implementing all protections required by the Data Privacy Directive would have significant economic and non-economic costs.\textsuperscript{55} The European Union responded by emphasizing its significant unease with the lack of centralized enforcement authority in the U.S. regulatory scheme, which could leave E.U. citizens "without a suitable U.S. authority to turn to if someone breaks the rules."\textsuperscript{56} Because most U.S. laws impacting privacy responded to specific abuses and practices in individual industries, within one company "the same types of personal information may be subject to different regulatory controls."\textsuperscript{57} The implementation of the Data Privacy Directive and corresponding E.U. Member State legislation between 1998 and 2000 forced the United States and Europe Union to address the disparity between their privacy regimes.

Faced with the loss of billions of dollars in annual transactions if data flows from the European Union were restricted, U.S. companies, represented by the U.S. Department of Commerce, entered into negotiations with E.U. officials to create a bridge between the two regulatory schemes.

\textsuperscript{50} Assey & Eleftheriou, supra note 12, at 146.
\textsuperscript{51} Council Directive 95/46, supra note 38, art. 28.
\textsuperscript{52} Zaidi, supra note 33, at 172.
\textsuperscript{53} Id.
\textsuperscript{55} Clear, supra note 25, at 987.
\textsuperscript{56} Id.
\textsuperscript{57} Ritter et al., supra note 11, at 96.
The resulting “Safe Harbor” framework, announced in July 2000, was intended to allow U.S. companies to fulfill the “adequate” standard of protection mandated by the Data Privacy Directive while maintaining the traditional U.S. approach of self-regulation.

As former Department of Commerce official David Aaron, who led the U.S. team of negotiators, explained, the Safe Harbor represented a conscious choice by the United States to avoid, effectively, “apply[ing] the E.U. Directive in the [United States]. What we were prepared to do was issue guidance to the American business community on how to conduct commercial relations with other countries.” The Safe Harbor invested the authority to enforce its provisions in the FTC and U.S. Department of Commerce, simultaneously addressing the European Union’s unease about decentralized enforcement and domestic industry concern about E.U. officials exercising jurisdiction over U.S. companies.

Under the Safe Harbor, participants have two options for ensuring the adequate protection of consumer data: self-regulation and self-certification. A company choosing the former option must join a recognized, U.S.-based self-regulatory privacy program, such as TRUSTe or BBBOnline, that adheres to the principles outlined in the Safe Harbor. One choosing the latter option must self-certify that it follows principles consistent to those provided in the Data Privacy Directive. Under the Data Privacy Directive, a company adopting the latter approach essentially commits itself to the jurisdiction of the European Union if issues arise concerning its handling of data from E.U. Member States. Alternatively, self-certifying businesses

---

61 Ritter et al., supra note 11, at 100.
63 Ritter et al., supra note 11, at 101.
64 Id.
65 Id.
may negotiate contracts for the transfer of data with the European Union on a case-by-case basis. Although that option would seem to be more in line with the U.S. free-market approach to privacy, the costs of compliance may be too great to make it a realistic choice for most U.S. companies. Most multinational companies based in the United States “would have to negotiate over thousands [of] such contracts” in order to continue normal business transactions. Faced with that possibility, U.S. companies might decide that participation in the Safe Harbor is more efficient (and more likely to protect their interests, should any conflicts arise).

In addition to reconciling conflicts between the U.S. and E.U. approaches to privacy regulation, the Safe Harbor negotiations also exposed an important weakness of the Data Privacy Directive—at least from the perspective of innovative U.S. businesses. First introduced in 1995, before the Internet became integral to the operation of domestic and international business, the Data Privacy Directive to a large extent failed to take into account emerging information technologies that changed the nature and processes of the data being regulated. In contrast, as was discussed in Section II.B, infra, most U.S. privacy laws enacted in the 1990s specifically responded to such innovations. As former Department of Commerce official Aaron explained, “the Europeans had to recognize that [they] were trying to adopt the Directive to the most advanced information economy on earth,” which meant that “the Safe Harbor [provisions] had to be more flexible and address real world information practices on a reasonable basis.”

Safe Harbor participation, which was slow to catch on in the program’s first two years, has grown recently. Still, it falls far short of including a majority of the U.S. companies who would suffer severe, adverse effects were data transfers from the European Union to be blocked. According to the Department of Commerce Safe Harbor website, as of October 2006, more than 1000 companies were participating in the

---

66 Aaron Testimony, supra note 60.
67 Id.
68 See id. (noting that the Data Privacy Directive “was conceived . . . when there was no World Wide Web and information technology was dominated by mainframe computers, not distributed information networks, laptops, and digital assistants. As a result, the Directive is often rigid or silent in dealing with privacy issues growing out of new technology and business models. Many European States have had great difficulty translating it into domestic law.”).
69 Id.
70 Only 40 companies enrolled in the Safe Harbor in its first six months; of those, only Hewlett-Packard and Dun & Bradstreet were “large multinational” companies. The other original participants were “generally either small to medium enterprises with privacy issues arising from business-to-consumer transactions, or self-regulatory organizations who are in the business of providing organizations with privacy compliance services.” Assey & Eleftheriou, supra note 12, at 147–48.
program. Of those, more than 190 (or approximately twenty percent) were listed as having “not current” certification status, though none had been cited for “persistent failure to comply” with the Safe Harbor Principles. Furthermore, the list makes it clear that not all Safe Harbor participants use the program for comprehensive coverage of the data they handle. Many specify which subsets of data processing they enrolled to cover, including data processed or maintained offline, online, or manually; or for human resources or clinical operations functions.

U.S. officials have recently raised concern that continued lackluster participation in the program might encourage the European Union to reconsider whether the Safe Harbor really mirrors the letter and spirit of the Data Privacy Directive. Critics of the Safe Harbor (not limited to E.U. officials) have pointed out a number of weaknesses (or potential weaknesses) in the program. First, the Safe Harbor does not centralize the administration and enforcement of privacy law writ large. Second, it does not provide a private right of action to respond to transgressions by participating companies. That does not mean that no remedy is available for such violations. Companies that violate the Safe Harbor are subject to discipline by the FTC; and consumers may potentially bring class action suits for fraud or misrepresentation against any companies that misuse personal data. Despite recognition that the Safe Harbor does not preclude alternatives, or that closing the regulatory gap between the United States and European Union might require its revision, thus far, no parties have demanded that the program be abandoned.

E. U.S. Privacy Legislation After the Safe Harbor

The concerns that prompted the enactment of sector-specific privacy legislation in the 1980s and 1990s, as well as those that led to the creation of the Safe Harbor, focused renewed legislative attention on consumer data privacy beginning in 2000. In February of that year, for instance, several members of Congress joined to create the Congressional Privacy Caucus. Issues highlighted in the Safe Harbor negotiations, as well as

---

72 Id.
73 Id.
76 Assey & Eleftheriou, supra note 12, at 158.
77 Zaidi, supra note 33, at 189. Senators Richard Shelby of Alabama and Richard Bryan
Congress' inability to impose stringent privacy requirements on the banking industry, spurred the founding members of the Caucus to educate their colleagues and advocate for additional legislation. Although emphasizing the traditional U.S. free-market approach to privacy regulation, the Caucus promoted four tenets for the handling of personal data that echoed the internationally established "fair information principles" that:

1) individuals be informed when private firms or government agencies collect and/or disclose personally identifiable information; 2) individuals have a right to access their personally identifiable information and have the ability to correct it; 3) individuals must [give] consent to a private company or government agency before it can disclose the individual's personally identifiable information; [and], 4) federal privacy laws do not preempt stronger state privacy laws.

The final tenet parallels the E.U. approach to implementing the Data Privacy Directive, in that the Directive provided a baseline standard for E.U. Member States, who could establish higher standards in their implementing legislation. The Congressional Privacy Caucus, similarly, advocated that states should be permitted to enact more stringent laws to protect the privacy and security of their citizens' personal data. The impact of the federal-state balance, however, is more likely to create conflicting liabilities in the United States, which has twice as many states as the European Union does members.

F. Recent State Legislative Efforts to Protect Consumer Data

Several states have indeed taken the opportunity to enact data privacy laws more stringent than those created by Congress. Some of these laws grant citizens a general right to privacy, though courts have restricted that right to torts such as intrusion and the "public disclosure of private facts." Other state laws explicitly codify those common law privacy torts. Some
states have mirrored the federal approach to privacy by enacting sector-specific privacy legislation.\(^{86}\) Furthermore, states such as California, Minnesota, North Dakota, and Vermont have enacted laws during the past decade that embody the original “fair information principles” and even include some of the central principles of the Data Privacy Directive. For instance, Minnesota’s Internet Consumer Privacy Act, enacted in 2002, reflects fair information practices also incorporated into the Safe Harbor;\(^{87}\) and Vermont’s health care records law has an “opt-in” measure similar to that included in the Safe Harbor Principles and the Data Privacy Directive.\(^{88}\) Several states have enacted legislation imposing particularly stringent regulations on the financial services industry, for instance requiring “opt-in” or “opt-out” provisions\(^ {89}\).

At the time that U.S. Department of Commerce officials were negotiating the Safe Harbor, debate began in Congress over yet another law that would control an industry’s treatment of consumer data: the Gramm-Leach-Bliley Act (“GLBA”).\(^ {90}\) GLBA amended the Bank Holding Company Act of 1956 to create a new class of financial services company, the “financial holding company,” which may engage in any “financial activity” or other activity reasonably related to financial services.\(^ {91}\) The concurrent development of the Safe Harbor and GLBA created a conflict for the U.S. financial services industry, essentially forcing its members to choose in which regulatory framework’s development they wished to participate.\(^ {92}\) Perhaps sensing greater potential to produce a favorable outcome in the latter legislation, the industry was largely absent from the Safe Harbor debates.\(^ {93}\) Financial services companies may have hoped that the European Union would deem the GLBA’s privacy protections, like the Safe Harbor, to provide the adequate level of privacy protection required for data to be transferred from E.U. Member States. Unfortunately for those countries, GLBA has never been declared adequate under the Data Privacy Directive.

GLBA imposed significant privacy requirements on financial services companies.\(^ {94}\) Regulations promulgated under Section 501 of the act mandate “safeguards” for financial services companies’ customer data.\(^ {95}\)

\(^{86}\) Id.
\(^{87}\) Tallman, supra note 74, at 762.
\(^{88}\) Zaidi, supra note 33, at 193–95.
\(^{89}\) Ritter et al., supra note 11, at 107–08.
\(^{92}\) Tallman, supra note 74, at 765–65.
\(^{93}\) Id.
\(^{94}\) Id. at 748.
Any company subject to GLBA’s provisions must implement and maintain a security program tailored to the company’s “size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.”\textsuperscript{96} A company’s security program must not only guarantee the confidentiality and security of customer information, but also protect against both (1) anticipated threats to that security and confidentiality and (2) unauthorized access of customer data that could cause “harm or inconvenience to any customer.”\textsuperscript{97} The development and maintenance of a security program compliant with the regulations includes designating company personnel responsible for the security and confidentiality of customer information, identifying potential risks that could result in the “unauthorized disclosure, misuse... or other compromise” of customer information, and periodically evaluating and updating the security program to address identified existing or potential risks.\textsuperscript{98} Thus, the GLBA failed to give the financial services industry a truly viable alternative to the Safe Harbor.\textsuperscript{99}

The enactment of GLBA and creation of the Safe Harbor encouraged greater federal coordination to protect the privacy and security of consumer data. Failure to comply with either set of provisions may constitute an unfair or deceptive trade practice under the Federal Trade Commission Act (“FTC Act”), thus inviting FTC enforcement actions.\textsuperscript{100} FTC analysis of whether a company is compliant with the requirements of the Safe Harbor and other privacy laws under which the FTC has jurisdiction embodies many of the basic principles of the Data Privacy Directive and its international predecessors.\textsuperscript{101} The FTC deems a company that adheres to certain standards of notice, consent, access, data integrity and security, and enforcement and redress to satisfy the Data Privacy Directive’s “adequate” protection requirement.\textsuperscript{102}

The FTC’s use of its enforcement powers, however, has thus far been minimal. In November 2004, the FTC brought its first charges for non-compliance with its GLBA Safeguards and Privacy rules.\textsuperscript{103} The FTC

\textsuperscript{96} Id. § 314.3.
\textsuperscript{97} Id.
\textsuperscript{98} Id.
\textsuperscript{99} Tallman, \textit{supra} note 74, at 748. Despite these “Safeguards,” one of the Congressional Privacy Caucus’s first actions was to voice concern that GLBA provided “inadequate” protection to consumer privacy. \textit{Fearsome Foursome Forms Congressional Privacy Caucus}, \textit{supra} note 77.
\textsuperscript{100} 15 U.S.C. § 45(a) (2000). Under Section 5 of the Act, which prohibits “unfair or deceptive acts or practices,” the FTC may be able to prosecute companies who fail to comply with its own privacy policy. Tallman, \textit{supra} note 74, at 762.
\textsuperscript{101} Zaidi, \textit{supra} note 33, at 190.
\textsuperscript{102} Id. at 190–91.
\textsuperscript{103} Press Release, Fed. Trade Comm’n, \textit{FTC Enforces Gramm-Leach-Bliley Act’s
charged two mortgage companies—Nationwide Mortgage Group, Inc., and Sunbelt Lending Services, Inc.—with violations of the Safeguards provisions for failure to enact “reasonable policies and procedures to ensure the security and confidentiality of customer information,” including customers’ names, social security numbers, credit histories, bank account numbers, and income tax returns.\textsuperscript{104} Both companies failed to provide adequate privacy notices to customers.\textsuperscript{105} In publicizing these charges, the FTC was careful to clarify that the complaints only indicated that the agency had “reason to believe” the companies had violated provisions of GLBA, rather than a conclusive finding that such a violation had occurred.\textsuperscript{106}

The Safe Harbor, GLBA, and other U.S. legislation passed subsequent to the Data Privacy Directive reinforce the U.S. adherence to its traditional market-based approach to privacy regulation. As two Brookings Institution officials emphasized, “[t]he absence of generic privacy legislation in the United States is not an indication that privacy lacks importance, but instead reflects the fact that the Constitution and legislatures at both the federal and state levels also value competing policy objectives.”\textsuperscript{107} Other supporters have pointed out that the U.S. approach “reflects the U.S. resistance to impose heavy burdens on business and the American preference for commercial freedom over mandated privacy.”\textsuperscript{108} Despite the more ambitious scope of the Safe Harbor, those policy objectives remain the dominant force in the U.S. approach to protecting consumer data, as is evident in the most recently proposed legislative additions to the regulatory framework. The next part section of this comment will discuss a few of those legislative proposals.

III. THE 109TH CONGRESS’ PROPOSED CHANGES TO THE U.S. REGULATORY FRAMEWORK

Spurred by requests to increase the protection of consumer data, members of the 109th Congress introduced a handful of bills that would alter U.S. companies’ obligations to consumers—and impose penalties for any resulting failures. Although the proposed bills have a common impetus, and although each responds at least in part to the standard established by the Data Privacy Directive, their foci and reach vary

\begin{footnotes}
\item[105] Id.
\item[106] Id.
\item[108] Gladstone, supra note 15, at 25.
\end{footnotes}
significantly. Generally, each of the proposed bills falls into one of three categories. First, some bills would create new security measures that apply to more than one industry. The 2005 Privacy Act, introduced by Senators Specter and Leahy in June 2005, is the leading example of this type of legislation. Second, another group of bills would amend existing legislation (mostly applicable to the financial services and closely related industries). This approach is embodied by the Financial Data Protection Act of 2005 ("Data Protection Act"), introduced by Representative Steven La Tourette of Ohio and Senator Tom Carper of Delaware, which would amend the FCRA to impose data security requirements on companies handling financial and related consumer data.\textsuperscript{105} Third, some bills address specific transactions or practices that result in the theft of consumer data. Bills such as the 2005 Privacy Act and Data Privacy Act have incorporated many of the most important elements of the third type of legislation. Accordingly, bills from the first two categories have the greatest potential to address concerns remaining after the creation of the Safe Harbor. The following analysis of the 109th Congress’ response to the Data Privacy Directive and shortcomings of the Safe Harbor will thus focus on the 2005 Privacy Act and Data Protection Act. Because the impact of bills such as the Data Protection Act would be limited primarily to the financial services industry, analysis of legislative alternatives also will focus on that industry where applicable.

A. The 2005 Privacy Act

The 2005 Privacy Act, clearly responding to public concern, emphasized the threat of identity theft posed by the improper use of data. The bill’s introductory findings section highlighted the fact that that more than nine million Americans were victims of identity theft in 2004, and proposed that “individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities.”\textsuperscript{110} Perhaps the most broad-reaching of the proposed bills, the 2005 Privacy Act addresses three major sets of concerns related to consumer protection: responding to the theft or improper handling of consumer data, monitoring data collection by large companies, and increasing the accountability of the federal government for its use of citizens’ data.

First, the 2005 Privacy Act would create a specialized scheme of civil and criminal penalties for identity theft and related “violations of data privacy and security,” and would provide resources for state and local law

---


enforcement agencies to pursue violators. The bill proposes specialized responses to incidents of identity theft generally involving (1) fraud or criminal activity, (2) organized crime, and (3) the concealment of violations of consumer data security. Violators would be subject to fines, jail sentences, or both, subject to proposed changes to the Federal Sentencing Guidelines. In addition to preventative measures, the bill also proposed new methods for responding to data security breaches and identity theft. It would create specific courses of action to be followed in the event of a large-scale data security breach. In particular, parallel to requirements of the Data Privacy Directive, the bill includes requirements for notifying individuals whose personal data has been lost or compromised.

Second, the 2005 Privacy Act would establish processes to be followed by companies collecting and using personal data from 5000 or more consumers. The bill would subject those “data brokers” to restrictions and regulations similar to those in effect in the European Union, with additional measures made applicable only to the largest-scale data handlers.

Finally, the 2005 Privacy Act would increase the federal government’s responsibility to handle data properly by enhancing the regulations concerning federal government use of commercial databases. These provisions would apply to any federal contract with a “data broker” worth more than $500,000. The bill would further require agencies intending to enter into such contracts to conduct “privacy impact assessments” before commencing the projects. Each of the primary federal agencies would be required to appoint a Chief Privacy Officer to ensure the agencies’ compliance with the bill’s requirements. Federal agencies wishing to use individual screening programs would have to receive Congressional authorization first. By creating provisions for the federal government as stringent as those applicable to private actors, the 2005 Privacy Act mirrors an important characteristic of the Data Privacy Directive, which does not distinguish between private and public actors in its expectations for the

---

111 Id.
112 Id.
113 McCullagh, supra note 4.
115 Id.
116 Id.
117 Id.
118 McCullagh, supra note 4. The requirement would apply only to federal agency use of a commercial database consisting “primarily” of U.S. citizen information. Id.
119 Id.
121 Id.
122 Id.
123 McCullagh, supra note 4.
proper use of personal data.

B. The Data Protection Act

Compared to the 2005 Privacy Act, the bills proposing amendments to the FCRA are much more limited in scope, at least insofar as the industries to which they would apply are concerned. The Data Protection Act, introduced in the House of Representatives in October 2005 and in the Senate two months later, would impose on credit reporting and related financial institutions the duty to create and maintain “reasonable policies and procedures to protect the security and confidentiality of sensitive financial information” whose misuse might result in harm to the consumer. Like the 2005 Privacy Act, the Data Protection Act would require companies collecting and using consumer data to investigate and address any leaks or other mishandlings of such data, with an eye toward preventing identity theft.

Two important distinctions between the Data Protection Act and 2005 Privacy Act should be noted. First, the Data Protection Act would be more limited in scope than the 2005 Privacy Act. The Data Protection Act would provide for its provisions to be read in concert with those of GLBA, to ensure that the bills would not impose conflicting obligations upon financial services organizations. The 2005 Privacy Act, in contrast, would apply to companies regardless of their obligations under existing federal law. Second, the bills approach the issue of enforcement differently. As was discussed above, the 2005 Privacy Act would create a uniform scheme of civil and criminal punishments for violators, with penalties varying according to the degree of the offense committed in connection with the misuse of consumer data. The Data Protection Act, in contrast, would continue the traditional U.S. approach of sector-specific, decentralized enforcement. A series of agencies under whose purview financial institutions fall, including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission, and the Federal Deposit Insurance Corporation, would retain compliance oversight.

That diversified oversight scheme, established by the FCRA, would

---

124 Id.
125 Id.
126 Id.
127 Id.
128 Id. The other federal agencies charged with oversight of the financial services industry are the Office of Thrift Supervision and the National Credit Union Administration. Horn, supra note 27, at 89 n.3.
ensure that the agencies best positioned to identify issues within different financial services organizations have responsibility for ensuring their compliance. However, it also would leave open the possibility, which worried the European Union, that no agency will be able to respond to more complex issues within the industry—for instance, misuses of financial data by a company engaged in transactions involving the domain of multiple agencies. Furthermore, the Data Protection Act would permit a handful of federal authorities, including the Secretary of the Treasury, to create exemptions to the bill’s security requirements. As such, the enforcement scheme proposed by the Data Protection Act may fall short of satisfying the concerns made explicit by the European Union in the Data Privacy Directive about providing “adequate” protection to all consumers.

IV. THE 2005 PRIVACY ACT AND DATA PROTECTION ACT WOULD FAIL TO RESOLVE OUTSTANDING ISSUES ABOUT THE PROTECTION OF CONSUMER DATA

Although the legislation introduced by the 109th Congress would increase protection for the privacy of consumer data, none of the proposed bills would comprehensively address concerns expressed during the Safe Harbor negotiations and in the wake of recent major data breaches. The issues not addressed by current legislative proposals could prevent a meaningful reconciliation of the two regulatory regimes.

A. Issues Unresolved by the 2005 Privacy Act and Data Protection Act

First, none of the proposed bills would create a private cause of action for individuals whose data is mishandled. All enforcement authority would continue to reside in the federal government, with some models preserving the current division of power, which delegates responsibility to a handful of federal agencies. Second, none of the proposed bills would provide remedies for individuals residing outside the United States. That shortcoming would undermine guarantees made to the European Union by the U.S. Department of Commerce when it advanced the Safe Harbor Principles. The bills proposed during the 109th Congress thus far would address many serious concerns applicable only to domestic privacy, and would create a more secure atmosphere for the use and transmission of consumer data within the United States. However, none of them would

---


130 “I would like to confirm that we agree that privacy legislation should not apply differently on the basis of nationality, as provided for in paragraph 19(e) of the OECD guidelines and paragraph 70 of the explanatory memorandum and to assure you that if such legislation were proposed in Congress, we would work within the legislative process to avoid any such effects.” LaRussa Letter, supra note 59 (emphasis added).
satisfactorily resolve the conflict with the Data Privacy Directive that prompted the promulgation of the Safe Harbor Principles and poses a continuing threat to the uninterrupted transaction of international business by U.S. companies.

Third, none of the proposed bills would provide comprehensive coverage of critical U.S. industries. Some provisions, theoretically applicable to all U.S. companies that collect and use consumer data, would exclude important industries from their coverage. The 2005 Privacy Act, for instance, effectively would make universally applicable standards to which only financial institutions are currently subject (under the GLBA). However, that bill specifically would exclude from its requirements organizations subject to GLBA and the FCRA, as well as to HIPAA. This final issue reflects the evolution of business forms (a phenomenon not limited to the United States), under which a company operating several lines of business may be subject to the jurisdiction of more than one government agency.

Although the United States has a tradition of sector-specific regulation, as companies become increasingly sophisticated and organizationally complex, the more narrowly tailored regulations proposed by the 109th Congress might prove inadequate to address even purely domestic concerns about the collection and transmission of consumer data. Even if the European Union were to decide that the 2005 Privacy Act, Data Protection Act, or another new law provided “adequate” protection for consumer data, it would not foreclose the possibility of industry-specific obstacles. Any bill excluding individual industries, particularly the financial services industry or another equally dependent on constant data transfers, would leave open the possibility of sector-specific action by the European Union, which could impede or even obstruct entirely that industry’s critical transactions.

The potential for such interruption, and its impact on U.S companies’ ability to conduct everyday international business transactions, arose in the

---

131 Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005); Financial Data Protection Act of 2005, S. 2169, 109th Cong. (2005). For instance, the 2005 Privacy Act enables individuals to address and correct issues with the accuracy of their personal information, and requires data brokers to inform individuals when previously deleted information is re-inserted into their personal accounts. The bill would also pre-empt state legislation addressing consumer control. In form, pre-emption parallels the E.U. approach that the Data Privacy Directive and other measures provide a foundation upon which Member States may build in enacting implementing data privacy legislation. In practice, the pre-emption provision might undermine the progress made by states such as California, Minnesota, and Vermont, which have led state action to protect consumers. See, e.g., Ritter et al., supra note 11, at 112.

late 1990s, eventually prompting the negotiation of the Safe Harbor.\textsuperscript{133} Many of the companies who stand to suffer such losses have closely connected domestic and international practices, and will be unable to avoid conflict in the conduct of everyday businesses transactions. A determination by the European Union that new U.S. legislation does not comply with the spirit of the Data Privacy Directive may lead the European Union to block the transmission of all personal data from its Member States to cease flowing to U.S. companies. Non-compliance may entirely obstruct everything from personal banking or brokerage transactions to U.S. companies’ ability to manage human resources functions involving their European-based employees.\textsuperscript{134} If the overarching weaknesses of any of the proposed bills persist after the enactment of new legislation, the possibility exists that U.S. and E.U. trade officials will have to work together again in the manner they did to agree upon the Safe Harbor Principles promulgated in 2000.

As Congress again considers each of the proposed bills, or perhaps in subsequent legislation, it may eliminate some or all of these outstanding concerns. However, as current legislation largely perpetuates the previous self-regulatory attitude taken by the United States to the concept of data security, and to the extent that companies have had input into proposed legislation, none of the bills currently under consideration are guaranteed to earn the European Union blessing of ensuring adequate privacy protection. And even without Congressional action, no guarantee exists that the transfer of personal data between the United States and E.U. Member States will continue unimpeded.

Several issues merit brief mention. First, several years after its creation, the Safe Harbor remains vulnerable to criticism. Critics of the program have contended that it fails to satisfy the Data Privacy Directive’s "adequate protection" standard. They have alleged that the introduction of dozens of federal and state laws concerning data privacy has critically undermined the Safe Harbor's efficacy.\textsuperscript{135} Second, even the European Union's regulatory regime has its flaws. For instance, current E.U.

\textsuperscript{133} See supra Part II.D. As the 1998 effective date of the Data Privacy Directive approached, U.S. companies became extremely nervous about whether they would be able to continue to conduct business in Europe. Because "no official body in either the European Union or any individual European nation had determined U.S. law to be 'adequate,' ongoing data transfers from Europe to the United States across a wide number of significant industries ... were in jeopardy of being disrupted." Ritter et al., supra note 11, at 99. U.S. companies, in an attempt to counter this perceived threat, claimed that the Data Privacy Directive violated international trade policy by constituting a non-tariff barrier to trade, because it would have the effect of "placing essential businesses and services of mutual benefit to both economies at risk." \textit{Id.}

\textsuperscript{134} George et al., supra note 43, at 738.

\textsuperscript{135} Ritter et al., supra note 11, at 112.
regulations do not provide for consumer notification when major breaches of data security do occur. Because the European Union lacks the authority to enforce all of its regulations against private companies, response to violations of data security is limited to private actions, and as a result may serve as less of a deterrent than would the bills currently under consideration in the United States.

B. Data Privacy’s Impact on the U.S. Role as a Global Business Leader

It is worth noting that the continued debate over privacy regulation reflects, and takes place in the context of, a constant competition for the domination of global business. As the United States emerged and maintained its status as a global economic leader, its businesses have been used to dictating the rules and regulations with which its global counterparts were forced to comply in order to be competitive. The European Union’s regulatory scheme has presented a serious challenge to U.S. global commercial dominance. As the European Union continues to impose the most stringent regulations, to some extent, U.S. businesses have been forced to adapt their practices to comply with those standards, and the United States is ceding some of its leadership.

The European Union’s enforcement of its Data Privacy Directive against non-Member States demonstrates its increased global business leadership. The force with which the Data Privacy Directive is being enforced may reflect past frustration on the part of E.U. Member States with the degree to which the United States directed other countries’ domestic policies through its own global business leadership. Furthermore, developing economies interested in competing with current commercial superpowers have most closely followed the European Union’s leadership in setting their own regulations. Alignment with the European Union regulatory framework may provide those countries with “an important bridge towards increased economic opportunities with the lucrative [E.U.] marketplace” and allow their companies to handle data originating in the European Union without the potential for expensive disruptions. Additionally, those countries may have been motivated by the conflicts evident in the debates over the Safe Harbor principles.

Finally, the balance of power in those developing economies may more closely resemble that in the European Union, further recommending

136 Clear, supra note 25, at 981.
137 Id.
138 George et al., supra note 43, at 736.
139 Ritter et al., supra note 11, at 104-05.
140 Id. at 104. For instance, in the United States there is considerable tension between the public and private sectors. In countries where less of this tension exists, “the enactment of a generic architecture for privacy law is significantly easier to accomplish.” Id.
the adoption of its regulatory framework. By contrast, the influence of the private sector in the United States has significantly complicated "the enactment of a generic architecture for privacy law." As Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, pointed out, as the Data Privacy Directive motivates more and more countries to adopt laws and regulations to protect consumer data, "[t]he United States is becoming increasingly isolated in the global debate over privacy protection." If that trend towards isolation continues, it may preclude the possibility for reconciliation of the U.S. and E.U. regulatory schemes.

C. Suggested Improvements to Current Legislative Proposals and Alternatives to Federal Legislation

The United States and European Union need to engage in further cooperative activity to eliminate or reduce the impact of competing liabilities that the new regulations will impose on U.S.-based financial services businesses. If the system is not amended, companies on both sides of the Atlantic—and around the world—will be haunted by the persistent possibility that the everyday conduct of international business transactions could come to a halt. Not only will basic transactions be delayed or entirely obstructed, but also U.S. companies will face increased difficulty in managing the human resources and related aspects of their business that involve European-based employees.

To respond to continuing concerns from both the United States and European Union, Congress should make a few key amendments to the existing legislative proposals.

First, Congress should revisit the "fair information principles" promoted by the Congressional Privacy Caucus, particularly to consider whether new bills should pre-empt state legislation on consumer privacy. As this comment discusses, a handful of states have led the way in strengthening consumer protection. Following the E.U. approach, Congress could enact new legislation that would serve as a baseline for data security. This would leave states free, as are E.U. Member States, to pass more stringent measures, which could have two benefits. First, setting a federal standard would preserve the traditional U.S. market-based approach to regulation. Second, from the European perspective, it would add a layer of enforcement to the U.S. regulatory scheme (presuming that states were given enforcement power, analogous to that granted to the DPAs in the

141 Id.
142 Id.
143 Rotenberg Testimony, supra note 31.
144 See infra at note 77.
145 See supra Part II.D; see also Ritter et al., supra note 11, at 108–09.
European Union). These similarities to the Data Privacy Directive's approach could help close the gap between current U.S. and E.U. regulatory policy, without forcing the United States to abandon its traditional approach to regulation.

Indeed, the key to resolving the conflict between the U.S. and European frameworks—with the former's relatively narrow conception of business operations because its regulations only concern "domestic operations and activities" and the latter's presumption that the majority of data transfers in the global economy will be transborder—may lie in state rather than federal regulations. As discussed in Part II.D, supra, several states have enacted legislation based on the "fair information principles" embodied in the Data Privacy Directive (and other international attempts to regulate consumer privacy). Assuming any future legislation does not foreclose the possibility of state-level regulation, it may present the best opportunity for closing the regulatory gap between the United States and European Union. At the same time, it would preserve the market-based approach traditionally utilized in the United States, while encouraging greater protection for consumers. U.S.-based companies with customers in multiple states would have to comply with the most stringent laws in order to avoid domestic liability. Alternatively, they would have to segregate all customer data according to the laws affecting it, an approach that would be expensive and difficult to self-audit.

In addition to giving serious consideration to the question of pre-emption, Congress also could add to any new legislation provisions mandating that every U.S. company engaged in international consumer data transactions participate in Safe Harbor-approved programs. Insofar as the European Union seems to have accepted the Safe Harbor in practice, this would add to the guarantee that no data transactions would be interrupted by E.U. officials. U.S. companies, however, may have a mixed response to this type of proposal. Major industries, including financial institutions, have repeatedly emphasized the value they place on the current U.S. regulatory approach, and might be able to secure significant delays in implementation for any mandatory Safe Harbor participation. On the other hand, increased participation in self-regulatory programs might leave more control with industries and the market—and would therefore be more true to the traditional U.S. approach. The most accurate gauge of industry response to either of these proposals would be to include it in the legislation being considered by the current Congress.

146 Ritter et al., supra note 11, at 98.
147 Id.
148 Id.
149 The 2005 Privacy Act would pre-empt state legislation on the protection of consumer data. See supra Part III.A.
Even if the United States does not enact more stringent regulations, the Data Privacy Directive and recent incidents concerning the loss or misuse of data have caused U.S. industries and consumers to pay much more attention to the issue. While states are free to enact harsher regulations, it may be to companies’ disadvantage to maintain the current regulatory framework, where compliance and liability may be based on fifty different sets of laws, each more stringent than federal requirements, even if those laws do not place enforcement authority with any federal agency comparable to one of the European Union’s DPAs.

IV. CONCLUSION

As Electronic Privacy and Information Center Executive Director Marc Rotenberg explained, the European Union’s Data Privacy Directive is not only a challenge for U.S. businesses participating in today’s global economy but also “a reminder that our privacy laws are out of date and that there is much work to be done . . . to ensure the protection of [consumer privacy]. Further action against the [Directive] will not make the privacy concerns in the [United States] go away.” 150 To an extent, U.S. legislative and regulatory actions since the enactment of the Data Privacy Directive have done some of that much-needed work. First, the Safe Harbor Principles promulgated by the U.S. Department of Commerce in 2000 were an important step towards unifying domestic expectations for the protection of data privacy. Those principles affirmed the traditional U.S. self-regulatory approach to privacy regulation while attempting to ensure that the disparity between the U.S. and E.U. approaches to such regulation would not create insurmountable obstacles for U.S. companies engaged in transatlantic data transfers. Second, Congress has continued to examine the issue of data privacy, prompted largely by public demand in the wake of several highly publicized incidents of data loss and growing concerns about identity theft.

As a response to domestic concerns, proposed bills including the 2005 Privacy Act and Data Protection Act represent progress towards more comprehensive protection for the privacy of U.S. consumers’ personal data. As a response to the European Union’s concern about the adequacy of U.S. privacy protection, however, they may yet fall short. First, much of the proposed legislation, including the 2005 Privacy Act, would exclude the financial services industry and related industries, which stand to lose the most if data transfers from the European Union are interrupted. Second, the proposed legislation also lacks relief for non-U.S. citizens whose data is mishandled by U.S. companies leaving unanswered one of the European Union’s primary concerns about the U.S. regulatory framework. Third, the

150 Rotenberg Testimony, supra note 31.
Data Protection Act and other proposed amendments to existing legislation would be industry-specific, leaving open the possibility that the European Union could interfere with auxiliary transactions still critical to U.S. companies’ ability to conduct their everyday business.

Perhaps the best approach, therefore, is to view the legislation proposed during the 109th Congress as the first step towards both improving the status of data security within the United States and ensuring that U.S. companies can continue to do business with international clients without impediment. Were Congress able to combine the measures proposed by the 2005 Privacy Act and as amendments to the FCRA, they might create a bill that would address both sets of concerns. Thus far, legislation proposed by the 109th Congress reflects the need for continued cooperation between the United States and European Union to ensure that companies on both sides of the Atlantic—and around the world—are able to transact everyday business unimpeded while providing sufficient protection to the individuals whose data they utilize.