I. INTRODUCTION

In the age of global trade through online commercial transactions, privacy is becoming a major issue in relation to the dissemination and protection of personal data. In the context of trade relations between the United States and the European Union ("EU"), online privacy issues are emerging in light of the widespread differences in privacy regulation between the two entities. These differences involve compliance with privacy standards relating to the protection of personal data.

Privacy regimes among various nations exist in either a comprehensive or sectoral fashion. Under Directive 95/46 EC ("Directive"), the EU employs a comprehensive approach that binds all EU member states to implement "adequate" protections of personal data used in commercial transactions.[1] In contrast, the U.S. employs a sectoral approach that involves less privacy protections.[2] U.S. companies engaging in online commerce with the EU are thus facing increasingly rigorous compliance standards. If such EU standards are not met by a U.S. company, penalties in the form of legal enforcement actions may result.

With regard to online commercial transactions, the EU utilizes strict privacy standards for non-EU entities accessing personal data from EU member states. The reason for introducing such standards is to curb misuse of personal data belonging to EU parties. Having extensive trade links with a dynamic and increasingly wired EU market, the U.S. is expressing concern over potential disruptions in trade that would impact

---

[1] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, *The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, available at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 30, 2003) [hereinafter *Directive 95/46/EC*].

[2] Department of Commerce, *Safe Harbor Overview, available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 30, 2003) [hereinafter DOC].

significantly on U.S commerce. This is because U.S. companies must comply with more rigorous privacy standards as set in the Directive. In allaying these fears, the U.S. and the EU conducted negotiations, resulting in the Safe Harbor agreement ("Safe Harbor").[3]

Using the Directive's principles, the Safe Harbor creates a scheme by which U.S. companies comply with stricter privacy standards relating to the transfer of online personal data. With respect to U.S. privacy law, this Safe Harbor regime substitutes the predominant sectoral approach for a more comprehensive approach. Comprehensiveness within the U.S. privacy regime is gathering momentum partly due to the influences of both the Directive and Safe Harbor. As part of this comprehensive regime, U.S. federal agencies act as enforcement authorities in monitoring those U.S. companies collecting personal data from consumers.

This paper argues that five factors create momentum in gradually shifting U.S. privacy laws towards a comprehensive regime: (a) the influence of the Directive; (b) the influence of the Safe Harbor; (c) increasing recognition by Congress that American consumers need more privacy protections; (d) increased privacy protections by States; and (e) concerns over potential disruptions in U.S-EU trade relations. Much of this paper will describe how the Safe Harbor draws from the Directive's principles in fostering comprehensiveness among companies involved in the program.

II. COMPREHENSIVE VS. SECTORAL APPROACHES

Privacy approaches between the U.S. and the EU differ substantially. Using the Directive, the EU approach involves comprehensive privacy protections for consumers

[3] *Id.*

and businesses transferring personal data.[4] Comprehensive protections refer to a broad scheme of enforcing strict privacy standards ("adequate protection") that combines all aspects of privacy law found in various industries under one overarching regime.[5] Within the EU, this regime requires all member states to follow general principles of privacy protection (espoused under the Directive) by adopting similar forms of legislation to aid enforcement. The implementation of comprehensive protections involves cooperation between EU authorities and private industry in order to maintain consistent privacy standards. An essential feature of comprehensive protections includes rights of redress for parties whose personal data are mishandled by companies not complying with such consistent standards. Thus, comprehensive protections obligate all member states to implement specific rules for entities transferring any personal data.[6]

An example of a Directive's specific rule meeting the "adequate" protection standard is when a party must disclose its own identity and information practices to individuals interested in presenting personal data.[7] Personal data generally include an individual's name, home and e-mail address, telephone and social security number, and credit card number.[8] Individual enforcement authorities known as Data Protection Authorities ("DPAs") oversee this standard throughout the EU.[9] The DPAs are

---

[4] International Trade Administration (Department of Commerce), *Safe Harbor Overview*, in Rebecca Herold, *The Privacy Papers* 619, 620 (CRC Press LLC 2002) [hereinafter *International Trade Administration*].
[5] *Id.*
[6] Directive 95/46/EC, *supra* note 1, *available at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 31, 2003).
[7] Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 Alb. L.J. Sci. & Tech. 57, 63 (2000).
[8] *Id.*
[9] Deparment of Commerce, *Frequently Asked Questions (FAQs) FAQ 5 The Role of the Data Protection Authorities, available at* <http://www.export.gov/safeharbor/FAQ5-DPAFINAL.htm> (last visited March 23, 2003) [hereinafter *DOC FAQ 5*].

authorized entities meant to ensure that the Directive's privacy standards are met within each EU member state, while also investigating and resolving privacy disputes.[10]

Under Article 28(1), the Directive delegates broad powers to the DPAs in completely restricting personal data flow between an EU entity and a U.S. entity when a privacy violation is committed.[11] Furthermore, if a U.S. company does not comply with advice given by a DPA to conform to "adequate" protections of personal data, the DPA will notify the Federal Trade Commission ("FTC") or other U.S. federal or state bodies with statutory powers to take enforcement actions.[12] The Directive also bestows substantial authority upon the DPAs to enforce privacy standards that are even more rigorous than the Directive itself.[13]

In contrast to the comprehensive approach, the U.S. follows a sectoral approach. The sectoral approach refers to a privacy scheme whereby federal and state governments regulate standards within specified sectors of the economy.[14] The U.S. privacy regime is sectoral in nature because privacy regulation involves a mix of federal/state legislation and self-regulation.[15] Whereas federal and state statutes govern the extent of personal data transfer under specific circumstances, self-regulation generally refers to U.S. companies enforcing their own privacy standards with little government involvement, but

---

[10] Blanke, supra note 7, (quoting U.S. Department of Commerce, *Frequently Asked Questions (FAQs) FAQ 5 The Role of the Data Protection Authorities*, *available at* <http://www.ita.doc.gov/td/ecom/FAQ5DPAsJune2000.htm> (last visited March 29, 2003)).
[11] See European Union Directive 95/46 EC, Article 28(1), *available at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 26, 2003).
[12] DOC FAQ 5, *supra* note 9, *available at* <http://www.export.gov/safeharbor/FAQ5-DPAFINAL.htm> (last visited March 29, 2003).
[13] Directive 95/46/EC, *supra* note 1, Article 28.
[14] DOC, *supra* note 2, available at <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 30, 2003).
[15] *Id.*

providing for some means of consumer redress.[16] A drawback with the sectoral approach is that it is difficult to enforce uniform privacy standards knowing that other industries not within the purview of government regulation have different standards. This makes it difficult to establish baseline privacy standards from which consumers and businesses alike can follow. But, with the growing influence of the Directive in terms of personal data transfer between EU and U.S. entities, this sectoral regime is gradually being replaced by self-regulation under a more elaborate scheme of monitoring personal data compliance.

Traditionally, privacy statutes were introduced by Congress to establish controls over the handling of consumer personal data by governmental sources rather than private entities. In recent times, however, Congress recognizes that American consumers are concerned about personal data protection from private sources. That is, American consumers feel that this sectoral approach does little to protect online personal data.[17] In gaining a sense of this concern, a project known as the Georgetown Internet Privacy Policy Survey revealed that 92.8% of U.S. commercial websites (randomly selected out of 361 websites) contained some type of personal identifying information, such as e-mail and postal address.[18]

(A) THE U.S. APPROACH PRIOR TO THE DIRECTIVE: COPPA AND THE FTC

Ensuring that privacy compliance exists requires legitimate enforcement from recognized authorities. Before the Directive, privacy enforcement in the U.S. was carried

[16] *Id.*
[17] *Id.* at 58.
[18] Georgetown Internet Privacy Policy Survey (GIPPS), *Frequently Asked Questions* (5/7/99), *available at* <http://www.msb.edu/faculty/culnanm/GIPPS/GIPPSFAQ.html> (last visited March 28, 2003).

through the Children's Online Privacy Protection Act ("COPPA").[19] Introduced by Congress in 1998, COPPA affords personal data protections similar to that of the Directive, but specifically for children using the Internet.[20] COPPA requires company websites receiving personal data from children under the age of 13 to post a privacy policy detailing the personal data they collect from young visitors.[21] Here, the protected information relates to user registration, or personal data that children reveal in chat rooms or posting services.[22] The website must also have a parental notification-and-approval policy in place.[23]

Enforcement of COPPA regulations was successfully administered by the FTC in fining San Francisco-based LookSmart Ltd. for $35,000 in redirecting visitors to a different site owned by the company.[24] The FTC argued that LookSmart Ltd. illegally collected personal data from children without getting permission from their parents.[25] Furthermore, the FTC noted that the LookSmart Ltd. website posted no privacy policy as required by COPPA.[26] COPPA thus illustrates how the FTC plays an active role in enforcing broader privacy protections within a U.S sectoral regime prior to the Directive. By fining U.S. companies for misusing personal data of American consumers, the FTC

---

[19] Computer World, *FTC assesses First Fines for Violating Online Kids' Priva y Law, available at* <http://www.computerworld.com/news/2001/story/0,11280,59778,00.html> (April 19, 2001) (last visited March 28, 2003).
[20] Federal Trade Commission, *New Rule Will Protect Privacy of Children, available at* <http://www.ftc.gov/opa/1999/9910/childfinal.htm> (last visited March 28, 2003) [hereinafter FTC Children].
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] FTC Children, *supra* note 20.
[25] *Id.*
[26] *Id.*

demonstrates its commitment in targeting U.S. companies for privacy violations relating to online commercial transactions.

(B) THE EU DATA PRIVACY DIRECTIVE AND ITS IMPLICATIONS ON U.S. BUSINESSES

Since the 1970s, EU member states are utilizing comprehensive privacy standards to safeguard European consumers and businesses.[27] Because EU member states initially followed a sectoral approach for personal data protection, the EU introduced stronger measures in the Directive to establish an over-arching privacy regime.[28] Initially proposed by the EU in 1995 and later adopted in 1998, the Directive provides a harmonized set of privacy standards within all industries that ensure the free flow of personal data between EU member states.[29]

Through Article 25, the Directive also creates specific guidelines in regulating the export of personal data from EU states to "third countries" only when such countries meet "adequate" protection standards.[30] Adequate privacy refers to compliance with strict standards set forth by the Directive whereby non-EU entities are required to provide personal data protections to EU entities supplying such data.[31] This compliance mechanism is influencing a change among U.S. businesses with regard to the handling of personal data. Realizing that EU privacy violations are enforced under the watchful eye of DPAs, U.S. companies hope to avoid a disruption in online personal data transfers during relevant transactions. In this regard, the Directive is compelling U.S businesses to

---

[27] John R. Vacca, *The European Data Protection Directive: A Roadblock to International Trade*, in Rebecca Herold, *The Privacy Papers* 569, (CRC Press LLC 2002).
[28] Directive 95/46/EC, *supra* note 1, *available at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 31, 2003).
[29] *Id.* at 569.
[30] *Id.* at 603.
[31] *Id.*

embrace EU-like privacy standards, and thereby modify their own personal data collection practices. As one commentator notes:

> The impact of the EU Directive demonstrates that the actions of other powerful states also shape U.S. regulation and business practice. Although the scope and content of U.S. regulation of data privacy protection depend substantially on domestic factors, EU regulatory policy significantly affects the playing field in the United States … External pressures from the European Union enhance the impact of U.S. internal pressures. The EU Directive prods U.S. businesses to change their behavior to avoid confrontations with EU regulators. It prompts U.S. legislators to press U.S. businesses to enhance their internal standards to avoid a regulatory conflict.[32]

The influence of the Directive upon U.S. privacy law is apparent in that a comprehensive regime with strict standards is finding its way into a sectoral regime. As one commentator states: "The European Directive exerts significant pressure on U.S. information rights, practices, and policies. The Directive facilitates a single information market place within Europe through a harmonized set of rules, but also forces scrutiny of U.S. data privacy."[33] With billions of dollars being exchanged in online transactions between companies in the EU and the U.S., it follows that non-compliance would prevent the flow of streamlined transactions. Another commentator illustrates the Directive's influence on U.S. privacy law in terms of impacting trade relations: "Brussels has gone so far as to give an ultimatum to Washington: adopt strong privacy laws, or stand the risk of losing countless trillions of dollars of business with Europe."[34]

Since U.S. businesses are accustomed to sectoral privacy laws with little oversight from a central enforcement authority, the challenge is to rearrange their methods of

---

[32] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 Yale J. Intl. L. 1, 80 (2000).
[33] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Hous. L. Rev. 717, 735 (2001).
[34] Vacca, *supra* note 27, at 570.

collecting personal data by guaranteeing "adequate" protection for EU entities. Conforming to such standards serves the dual purpose of helping U.S. companies avoid facing EU legal enforcement action, while preserving existing business contacts within the EU. To meet these challenges, it would be essential to find an appropriate compromise to resolve the U.S. EU privacy regime differences.

III. ENTER THE SAFE HARBOR: ACTING AS A SUBSTITUTE FOR COMPREHENSIVENESS IN THE U.S.

With different privacy regimes in place, the U.S. struck a political compromise with the EU to ease concerns expressed by both entities over potential disruptions in trade relations. This compromise known as the Safe Harbor is gradually incorporating comprehensive privacy standards (derived from the Directive) into a U.S sectoral-based system. The Directive influences the Safe Harbor by furnishing broad standards of "adequate" protections. Because of its nature as a voluntary agreement and not as official law, the Safe Harbor does not bind all U.S. states to embrace comprehensive privacy standards. However, on the corporate level the Safe Harbor replaces the sectoral approach with a comprehensive approach by requiring company compliance with specific principles of "adequate" protections of personal data. In this way, the Safe Harbor acts as an important precursor to the development of comprehensive laws within the U.S. private sector by emphasizing compliance with stricter privacy standards.

This Safe Harbor agreement was successfully negotiated between the Department of Commerce ("DOC") and the European Commission in July 2000.[35] A statement made by Robert LaRussa, the Acting Under Secretary of the International Trade

[35] International Trade Administration., *supra* note 4, at 619.

Administration, amply illustrates the overall purpose of the Safe Harbor: "The safe harbor is a landmark accord for e-commerce. It bridges the differences between EU and U.S. approaches to privacy protection and will ensure that data flows between the U.S. and the EU are not interrupted. As a result, it should help ensure that e-commerce continues to flourish."[36]

The Safe Harbor is thus a means for streamlining commercial activity using online personal data protections as a means for U.S. businesses to satisfy EU-like "adequacy" requirements. The link between the Directive and the Safe Harbor is that U.S. companies voluntarily joining the Safe Harbor are required to follow seven principles ("Principles") when transferring personal data with EU entities: (1) Notice; (2) Choice; (3) Onward Transfer; (4) Security; (5) Data Integrity; (6) Access; and (7) Enforcement.[37] Notice has three functions: (a) it informs the individual as to the purpose for which the data is being used; (b) it provides a means to contact companies for inquiries or complaints; and (c) it gives information on the types of third parties who have access to the personal data held by the online provider.[38]

Choice offers individuals the chance to: (a) 'opt out' if personal data is disclosed to a third party, or used for a purpose other than which it is originally intended; and (b) 'opt-in' for sensitive personal data (i.e. health, ethnic origin) which is disclosed to third parties.[39] Onward Transfer allows the transfer of personal data to third parties acting as an agent for the company collecting the data, provided that the company ensures that the

---

[36] Memo. from Robert Larussa, Acting Under Sec. of Intl. Trade Administration, to Colleagues, *available at* <http://www.export.gov/safeharbor/larussacovernote717.htm> (July 21, 2000) (last visited March 25, 2003).
[37] International Trade Administration., *supra* note 4, at 620-21.
[38] *Id.*
[39] *Id*.

agent complies with the Principles or is subject to the Directive.[40] Security requires companies to take reasonable precautions to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, or destruction.[41]

Data integrity requires that personal data be relevant for the purpose for which it is to be used.[42] Access allows individuals to review company records to correct, amend, or delete personal data that is inaccurate or too sensitive in nature.[43] Finally, enforcement demands that companies provide recourse mechanisms for individuals to resolve privacy disputes, and award damages.[44] These seven Principles represent a baseline standard from which U.S. companies collecting personal data from EU entities must follow to meet the "adequate" protection standard. Any U.S. company receiving personal data from an EU party without abiding by these Principles may face legal enforcement action either by a U.S. or EU authority, which may result in a court awarding damages to the EU party.[45] More importantly, however, personal data collected by U.S. companies during a commercial transaction will be terminated by U.S. or EU enforcement authorities.[46]

(A) DEVELOPING COMPREHENSIVENESS: STRUCTURAL ARRANGEMENT OF THE SAFE HARBOR

The structural arrangement of the Safe Harbor allows U.S. federal agencies to formally embody comprehensive standards similar to that of EU authorities. At the onset of joining the Safe Harbor, U.S. companies may choose between FTC or DPA

---

[40] *Id.*
[41] *Id.*
[42] International Trade Administration, *supra* note, at 620-21.
[43] *Id.*
[44] *Id.*
[45] Department of Commerce, *Safe Harbor Overview*, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 29, 2003) [hereinafter *DOC website*].
[46] Blanke, *supra* note 7, at 81.

enforcement for resolving privacy disputes. This manner of choosing bolsters the FTC's ability to enforce "adequate" protection standards within the U.S. The FTC takes on a role similar to that of the DPA by ensuring that companies handling personal data during commercial transactions meet the "adequate" protection standard.

By providing a choice between using either FTC or DPA enforcement mechanisms, the Safe Harbor invites U.S. companies to provide their own enforcement mechanisms (normally used in a sectoral approach) in order to meet the "adequate" standard. Although such an arrangement merges a sectoral-based principle with an EU requirement, the Safe Harbor still manages to incorporate some elements of a comprehensive scheme into a sectoral regime. Over time, U.S. companies familiarize themselves with such stricter privacy standards.

(B) DEVELOPING COMPREHENSIVENESS WITHIN U.S. COMPANIES: SELF-REGULATION AND SELF-CERTIFICATION

Ensuring that "adequate" privacy protections are enforced within the Safe Harbor, Self-regulation and self-certification are two methods of achieving this goal. When EU parties complain about the content and use of personal data, U.S. companies utilize specific procedures in a process known as self-regulation.[47] Self-regulation allows U.S. companies to create an independent means for resolving privacy disputes with EU parties, such as with dispute resolution.[48] If a U.S. company commits a privacy violation, an EU party is encouraged to settle the dispute within the U.S.[49] Thus, self-regulation

[47] *Id.* at 69.
[48] *Id.* at 70.
[49] DOC website, *supra* note 45, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 29, 2003).

provides a means to enforce "adequate" privacy protections with little governmental involvement.[50]

Apart from the Safe Harbor, the most common form of self-regulation in the U.S. involves online privacy seal programs, such as TRUSTe and BBBOnline.[51] The link between such programs and the Safe Harbor is that the seal programs assist U.S. companies in creating privacy policy statements that resemble Safe Harbor-like privacy standards.[52] The Safe Harbor uses these forms of self-regulation as part of its scheme to merge the traditionally U.S. sectoral approach within a more comprehensive EU-like regime. The incorporation of this procedure denotes flexibility in enforcement.

However, a major criticism regarding online privacy seal programs relates to implementation.[53] Pursuant to the *Online Privacy and Disclosure Act of 2000*, such programs normally display a distinct privacy seal on a U.S. company's website to prove that it is complying with the Principles.[54] The seal programs alert the EU consumer as to the information practices used by a U.S. company during an online commercial transaction. But the problem with seal programs, as indicated in a 2000 FTC Report to Congress, is that "[t]he seal programs have yet to establish a significant presence on the Web."[55]

Recently, however, more seal programs are being found on U.S. commercial websites. For instance, a seal program on the FTC's website shows a "Dewie e-Turtle"

---

[50] Blanke, *supra* note 7, at 69.
[51] Federal Trade Commission Report. *Privacy Online: Fair Information Practices in the Electronic Marketplace A Report to Congress* 6 (May 2000) [hereinafter *FTC Report*].
[52] *Id.*
[53] *Id.*
[54] *Id.* at 3.
[55] *Id.* at 6.

privacy seal.[56] The "Dewie" initiative encourages U.S. consumers and businesses to review FTC recommendations to safeguard personal data.[57] The FTC website also contains links to other privacy protection sites such as the National Cyber Security Alliance's StaySafeOnline.info.[58] The growth of website seal programs demonstrates the level of commitment by U.S. entities (like the FTC) to promote personal data protection schemes among American consumers and businesses.

The other means of joining the Safe Harbor is self-certification.[59] Under self-certification, a U.S. company sends a letter to the DOC stating its intent to voluntarily join the Safe Harbor, while also agreeing to cooperate with the DPAs in the event an investigation of privacy disputes is brought by EU parties.[60] This is an annual certification process assuring the DOC that a U.S. company will adhere to Safe Harbor privacy standards for personal data collection.[61]

By publicly declaring its intent to join the Safe Harbor, a U.S. company also agrees to post a detailed privacy policy statement on its website that purports to comply with "adequate" standards.[62] Nevertheless, U.S. companies are concerned about facing legal actions over privacy violations that they unknowingly commit under the Safe Harbor. Upon joining the Safe Harbor, U.S. companies may use either FTC or EU

---

[56] Federal Trade Commission, *Dewie E-Turtle Consumer Information*, *available at* <http://www.ftc.gov/bcp/conline/edcams/infosecurity/> (last visited March 29, 2003) [hereinafter *FTC website*].
[57] *Id.*
[58] *Id.*
[59] Department of Commerce, *Safe Harbor Overview*, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 29, 2003).
[60] FTC website**,** *supra* note 56, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 28, 2003).
[61] *Id.*
[62] *Id.*

enforcement bodies to resolve privacy disputes in case their own dispute resolution mechanisms do not suffice.[63]

Regardless of whether or not self-regulation or self-certification resolves a privacy dispute, these procedures involve significant contact with both U.S. and EU authorities. This system of administration ensures the implementation of more comprehensive privacy protection standards within the U.S by holding U.S. companies accountable for their actions. That is, when U.S. companies voluntarily join the Safe Harbor but commit privacy violations, little can be done to escape liability knowing that U.S. federal agencies and EU authorities are directly involved in overseeing compliance. In this sense, the Safe Harbor mimics the style of EU compliance for "adequate" protection.

(C) DEVELOPING COMPREHENSIVENESS: SAFE HARBOR REQUIREMENTS

Complying with the Safe Harbor's general requirements signals a U.S company's intent to meet EU adequacy requirements relating to personal data protections. If a U.S. company voluntarily joins the Safe Harbor, it must follow five general guidelines.[64] First, the company must comply with all seven Principles.[65] Second, it must review the fifteen frequently asked questions ("FAQs") prepared by the DOC.[66] Third, it must certify to the DOC that it has implemented the Principles, either publicly in the form of "self-

[63] DOC FAQ 5, *supra* note 9, *available at* <http://www.export.gov/safeharbor/FAQ5-DPAFINAL.htm> (last visited March 29, 2003).
[64] The Direct Marketing Association, *The DMA Safe Harbor Program: A Guide for Businesses*, *available at* <http://www.thedma.org/safeharbor/businesses.shtml> (last visited March 28, 2003) [hereinafter *DMA website*].
[65] *Id.*
[66] *Id.*

certification" or through "self-regulation".[67] Fourth, it must have available appropriate enforcement mechanisms, along with an independent third-party dispute resolution mechanism for privacy violations.[68] Fifth, it must continue complying with the Principles in good faith while participating throughout the Safe Harbor program.[69]

These requirements illustrate the commitment involved in joining a comprehensive regime like the Safe Harbor. Modifying data collection practices to conform to the Principles requires an understanding and acceptance of more comprehensive privacy laws designed to permit a highly regulated form of online commercial transactions. Cooperation with the DOC for reviewing FAQs and the notification requirement encourages a U.S. company to form a unique partnership with federal authorities. This partnership bears a striking resemblance to an EU entities' close dealings with a DPA. Since the sectoral approach has no such partnership, it follows that the Safe Harbor seems to foster a comprehensive-like approach by promoting cooperation between government and private industry in the scope of Safe Harbor privacy compliance.

(D) DEVELOPING COMPREHENSIVENESS: PRIVACY WEST AND DIRECT MARKETING ASSOCIATION

The Safe Harbor's influence in promoting comprehensiveness not only extends to Safe Harbor companies but also to the U.S. private industry, thereby encouraging U.S. companies to join the Safe Harbor. Companies are establishing various websites as a means to ensure compliance with EU adequacy standards. For example, Privacy West is a

[67] *Id.*
[68] *Id.*
[69] *Id.*

California business specializing in helping small to medium size businesses with Safe Harbor privacy compliance.[70] Realizing that companies are concerned over the costs associated with meeting Safe Harbor requirements, Privacy West creates practical methods for U.S. companies to establish privacy policies that conform to the Principles. Such methods include step-by-step instructions on how U.S. companies can self-regulate instead of self-certifying with the DOC.[71]

Other U.S. companies are actively promoting "adequacy" standards via the Safe Harbor. For instance, the Direct Marketing Association ("DMA"), the largest trade association for U.S. businesses involved in global marketing, operates a DMA Safe Harbor Program ("DMASHP").[72] DMA members include, among others, AT&T, IBM, the New York Times, and Proctor & Gamble.[73] This program helps DMA members create privacy policies on websites that conform to all Safe Harbor Principles.[74]

This program also helps U.S. companies by providing independent third-party dispute resolution mechanisms.[75] This type of assistance fulfills one of the five Safe Harbor general guidelines requiring companies to seek third-party dispute resolution mechanisms when privacy complaints are lodged against them by EU entities. The DMA's dispute resolution body satisfies EU entities by providing: (1) fair and unbiased

---

[70] Privacy West, *About Privacy West*, *available at* <http://www.privacywest.com/about.html> (last visited March 28, 2003).
[71] *Id.*
[72] DMA website, *supra* note 64, *The DMA Safe Harbor Program*, *available at* <http://www.the-dma.org/safeharbor/index.shtml> (last visited March 28, 2003).
[73] DMA website, *What is the Direct Marketing Association*?, *available at* <http://www.the-dma.org/aboutdma/whatisthedma.shtml> (last visited March 28, 2003).
[74] *Id.*
[75] *Id.*

decision-making; (2) an accessible means of filing a complaint; (3) resolution of a dispute in a timely manner; and (4) certainty in enforcing legal actions.[76]

The DMA also has a "Safe Harbor Line", which is a free consumer service offering advice on matters relating to privacy disputes between EU entities and U.S. companies.[77] In this way, U.S. companies educate the general public about unfamiliar privacy standards. If there is no resolution on a matter, the Safe Harbor Line staff directs EU consumer complaints to the DMA's Safe Harbor Program Committee for review.[78] This committee is composed of direct marketing experts and recognized consumer representatives.[79]

If this DMA body finds that a U.S. company clearly violates a Safe Harbor Principle, it may notify such a violation to the FTC and DOC, who then take appropriate legal action.[80] Moreover, sanctions are imposed on such U.S. companies by: (1) correcting or deleting inaccurate personal information; (2) reimbursing direct monetary damages to consumers; (3) suspending the company from the DMA Safe Harbor Program; and (4) generating publicity for non-compliance.[81] Once again, a unique mechanism of cooperation exists between a U.S. company and a federal agency (much like the EU privacy regime) in regulating strict privacy standards. The DMA program illustrates how one U.S. company supplements "adequate" privacy compliance in other U.S. companies.

---

[76] *Id.*
[77] *Id.*
[78] DMA website, *supra* note 73.
[79] *Id.*
[80] *Id.*
[81] *Id.*

The legal authority in the DMA Safe Harbor Program Committee derives from specific provisions in a contract.[82] For example, the DMA Safe Harbor Program Contract under section 9 notes:

> Participant's failure to comply with any and all remedies resulting from the DMASHP may, pursuant to the Safe Harbor, result in The DMA's notifying any known governmental entity or other self-regulation program in any country, including without limitation the Attorney General of any State, the United States Federal Trade Commission, any law enforcement agency, any other state or federal governmental agency with jurisdiction over this matter, or any foreign privacy authority or other foreign government authority, of Participant's non-compliance.[83]

The DMA program thus illustrates how legally binding obligations are imposed by the Safe Harbor on U.S. businesses. The language of the DMA contract suggests that not only will a U.S. company be disciplined by various U.S. federal authorities, but also by governments and foreign privacy authorities "in any country". The contract also indicates a close partnership that exists between the U.S. federal government, private industry, and foreign governments in promoting "adequate" privacy compliance. By providing assistance to U.S. companies not familiar with comprehensive privacy protections for personal data, the DMA program acts as a conduit for U.S. companies willing to conduct online commercial transactions with EU entities, while limiting the risk of committing privacy violations.

IV. INCENTIVE FOR U.S. COMPANIES TO JOIN THE SAFE HARBOR: TRADE RELATIONS

To gain a sense of the economic impact that privacy compliance has upon trade relations, trade in personal data between the U.S. and the EU in 2000 was valued at $120

---

[82] *Id.*

[83] DMA website, *supra* note 64, *The DMA's Direct Marketer's Guide to Compliance with the Safe Harbor Program for European Data*, *available at* <http://www.the-dma.org/bookstore/cgi/displaybook?product_id=000003> (last visited March 28, 2003).

billion.[84] The Safe Harbor's impact upon commercial activities within the U.S. acts as a warning for U.S. companies who resist changing current personal data collection practices when dealing with EU entities. Although U.S. companies are taking an understandably cautious approach in deciding whether or not to join the Safe Harbor, other companies such as IBM, Hewlett-Packard, and Microsoft are active participants in the program, giving them considerable leverage in an enlarging EU market.[85] It follows that in order to remain competitive in the EU market, U.S. companies must change their own data collection practices to comply with more comprehensive privacy standards. Not making these changes will affect their ability to transfer personal data necessary for commercial transactions.

Having U.S. companies comply with the Safe Harbor restores confidence in EU entities that suggests the U.S. is making a concerted effort to improve and actively enforce more comprehensive privacy standards. Joining the Safe Harbor also creates a presumption that U.S. companies provide "adequate" protection, as espoused under Article 25 of the Directive.[86] With the EU market representing almost 500 million citizens, U.S. companies are eager to maintain, if not increase, trade relations with the EU by actively promoting comprehensive privacy compliance. Aside from trade relations, the U.S. is also recognizing how personal data is becoming a sensitive issue among American consumers - one that impacts local online commerce. Congress reiterates this point by noting that: "Market research demonstrates that tens of billions of dollars in e-

---

[84] Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade* Commission, 70 Fordham L. Rev. 2777, 2779 (2002) (quoting Richard Raysman & Peter Brown, *International Privacy: Safe Harbor Protection for Personal Data,* N.Y.L.J. at 3 (2000)).
[85] DOC website, *supra* note 45, *The Safe Harbor List, available at* <http://www.ita.doc.gov/td/ecom/FRN2.htm> (last visited March 30, 2003).
[86] Lawrence D. Dietz, *Data Privacy Directive 95/46 EC: Protecting Personal Data and Ensuring Free Movement of Data*, in Rebecca Herold, *The Privacy Papers* 569, 603 (CRC Press LLC 2002).

commerce are lost due to individual fears about a lack of privacy protection on the Internet."[87]

V. THE SAFE HARBOR AS A SUBSTITUTE AND PRECURSOR FOR COMPREHENSIVENESS IN THE U.S.

Congress recognizes the need to introduce an overarching privacy regime. Even prior to the Safe Harbor, U.S. legislators felt that more concrete privacy laws should be enacted for the benefit of American consumers. Congress summarizes this sentiment in the *Electronic Privacy Bill of Rights Act* of 1999 by noting that: "A national privacy policy that relies in part upon industry self-regulatory initiatives, technological tools for consumers, and Government-backed protections is needed to foster future development of electronic commerce and to safeguard the essential rights of individuals with respect to collection and use of their personal data."[88]

Although the Safe Harbor is an attempt to resolve privacy regime differences between the U.S. and the EU, it establishes a baseline from which Congress can adopt more comprehensive privacy laws. This can be achieved by using the Principles as a common standard for individual states to safeguard personal data of consumers. Although privacy enforcement in the U.S is administered primarily through self-regulation in the private sector, a noticeable partnership is developing between the U.S. government and U.S. private entities to improve privacy compliance. As the DOC notes: "Private sector

[87] Sen. 2201, *Online Personal Privacy Act*, 107th Cong., 2nd Sess. 46 (Aug. 1, 2002) [hereinafter *OPPA*].
[88] H.R. 3321, *Electronic Privacy Bill of Rights Act,* 106th Cong., 1st Sess., 4 (1999).

self regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes."[89]

That is, if EU entities are dissatisfied with U.S. private sector enforcement for privacy violations, the U.S. government remains committed to carry through on the enforcement process. Considering that various U.S. state legislatures are adopting privacy laws in accordance with Safe Harbor-like standards, it appears that U.S. privacy law is being shaped in accordance with privacy standards in the Directive. Introducing comprehensive privacy measures illustrates the effort to administer greater privacy protections for U.S. entities, while ensuring streamlined commerce with EU entities. In the context of online commercial activity, the generous protections afforded by the Safe Harbor to EU entities beyond its jurisdiction influences the U.S. approach to adopt similar protections for American entities.

(A) DRAWING FROM THE DIRECTIVE: OPPA

Remedies function as a means to encourage U.S. companies to comply with strict privacy controls for personal data collection. The Safe Harbor prompted the U.S. to introduce legislation to provide compensation for U.S. citizens affected by privacy violations. The *Online Personal Privacy Act of 2002* ("OPPA") grants remedies to American consumers who provide personal data to U.S. companies that fall short of providing "adequate" privacy protection.[90]

---

[89] U.S. Department of Commerce, *Safe Harbor Overview, available at* <http://www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm> (last visited March 28, 2003).
[90] OPPA, *supra* note 87, at 15.

The OPPA distinguishes between sensitive and non-sensitive information.[91] For sensitive information (such as financial data, health records, ethnicity, or sexual orientation), the OPPA grants a private right of action in a U.S. district court if an internet service provider or commercial website operator inappropriately discloses such information.[92] Upon a showing of actual harm, an individual may recover monetary losses or $5000.[93] For repeated privacy violations of sensitive information, OPPA gives wide discretion to courts for increasing the amount of damages, but not in excess of $100,000.[94]

A comparison between the Directive and OPPA reveals how online providers are required to follow notice and consent requirements when handling personal data of users. For instance, Article 7 of the Directive states: "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent . . . ."[95] Under Section 102(b) of OPPA, "An internet service provider, online service provider, or operator of a commercial website may not – (1) collect sensitive personally identifiable information online, or (2) disclose . . . such information collected online, from a user of that service or website, unless the provider or operator obtains that user's consent . . ."[96]

OPPA thus demonstrates how Congress draws from the Directive to ensure "adequate" protection of personal data for U.S. citizens. As one speaker indicates in an OPPA Senate floor statement: "In this respect, the legislation is also similar to the two-

[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] Directive 95/46/EC, *supra* note 1, at 14.
[96] OPPA, *supra* note 87, at 50.

tiered approach taken by the European Union in which companies are required to provide baseline protections governing the use of non-sensitive information, and stronger consent protections governing the use of sensitive data."[97] This recognition by U.S. legislators for providing greater personal data protections for U.S. citizens is another instance that stronger privacy measures are being incorporated within U.S. privacy law.

(B) DRAWING FROM THE DIRECTIVE: CPPA

Aside from OPPA, other privacy statutes passed by Congress reveal a trend towards adopting comprehensive privacy standards. For instance, the *Consumer Privacy Protection Act* of 2000 ("CPPA") establishes privacy protections for online personal data by drawing statutory language from the Directive.[98] For instance, a striking similarity exists between the Directive and the CPPA regarding the Principle of Access. Under Article 12 of the Directive (Right of Access), "Member States shall guarantee every data right to obtain from the controller: . . . (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[99]

Likewise, under Section 102(c) of the CPPA (Access), "[a]n Internet service provider, online service provider, or operator of a commercial website shall … (2) provide a reasonable opportunity for a user to correct, delete, or supplement any such information maintained by that provider or operator;"[100] The similarity between the

---

[97] *Id.*
[98] Sen. 2606, *Consumer Privacy Protection Act*, 106th Cong. § 102, 11 (May 23, 2000) [hereinafter *Sen. 2606*].
[99] See Article 12 of the Directive 95/46/EC, *available at* <http:www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 30, 2003).
[100] Sen. 2606, *supra* note 98, at 12.

Directive and the CPPA exists in the statutory language such that online service providers are required to permit consumers to access and modify personal data. Both statutes grant the consumer considerable power to control the content and transfer of personal data during online commercial transactions.

The CPPA contributes to comprehensiveness in the U.S. by raising awareness to both the FTC and Congress about the growing importance of privacy protections affecting American consumers. For instance, section 307 of the CPPA requires the FTC to establish an *Office of Online Privacy* to study privacy issues related to e-commerce and the Internet.[101] This body submits annual reports to the Senate Committee on Commerce, Science, and Transportation, as well as the House of Representatives Committee on Commerce.[102] The Office of Online Privacy also recommends additional privacy legislation to Congress.[103] This process ensures that Congress is aware of concerns addressed by American consumers over privacy protections, while also signaling the need to promulgate stricter standards within the U.S.

Realizing that the FTC actively enforces comprehensive privacy standards, Congress is certainly attentive of consumer complaints of online privacy protections. In the context of the CPPA, Congress notes that: "[p]rivacy safeguards should be applied uniformly across different communications media so as to provide consistent consumer privacy protections."[104] In efforts to study online privacy issues affecting Americans,

[101] *Id.* at 35.
[102] *Id.*
[103] *Id.*
[104] *Id.* at 6.

Congress established a bi-partisan group known as the Congressional Privacy Caucus in February 2000 ("Caucus").[105]

The Caucus seeks to educate members of Congress on privacy issues such as consent, unauthorized access to personal data, and basic privacy protections for online commercial activity.[106] The Caucus also holds forums and discussion panels with privacy advocates and Internet companies to address privacy issues in the hopes of making important legislative proposals.[107] For instance, the issue of web bugs is eliciting the Caucus to question the use of invisible tracking methods to determine online transactional behavior.[108] To counter what it sees as a blatant misuse of such data, the Caucus seeks laws that limit the manner in which online companies gather and exchange personal data.[109]

(C) CONTRIBUTING TO COMPREHENSIVENESS: THE FEDERAL TRADE COMMISSION

Extraordinary changes led by the FTC are shaping U.S. privacy laws to encompass broader privacy standards. In November 1999, a joint effort between the FTC and DOC resulted in presenting a public workshop on "online profiling" by third-party advertisers.[110] This workshop educates the public about privacy issues, while also

---

[105] Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First* Century, 4 N.Y.U. J. Legis. & Pub. Policy 439, 459 (2000-01) (quoting Michele Masterson, *Privacy Fuels Government Efforts: Growing Internet Privacy Concerns Spur Politicians to Introduce New Legislation* (Mar. 9, 2000), *available at* < http://www.cnnfn.com/2000/03/09/technology/q_legislation/> (last visited March 30, 2003).
[106] *Id.*
[107] Senator Chris Dodd website, *Dodd Joins Congressional Privacy Caucus, available at* <http://dodd.senate.gov/press/Releases/01/0201.htm> (as of February 1, 2001) (last visited March 30, 2003).
[108] ADLAW, Hall Dickler Kent Goldstein & Wood, *Congressional Group to Coordinate Privacy Debate, Seeks to Prohibit Web Bugs, available at* <http://www.adlawbyrequest.com/legislation/WebBugPrivacyCaucus.shtml> (February 12, 2001) (last visited March 30, 2003).
[109] *Id.*
[110] FTC Report, *supra* note 51, at 5.

highlighting fair information practices in the scope of online advertising.[111] In December 1999, the FTC assembled an Advisory Committee on Online Access and Security, consisting of industry representatives, security specialists, and consumer and privacy advocates.[112] Convening in public meetings, this body advises the FTC about fair information practice principles within the U.S.[113]

In applying practical enforcement measures, the FTC identifies five core principles of privacy protection, as derived from the Organization of Economic and Cooperation of Development (OECD) Guidelines and the Directive.[114] These principles include: (1) Notice/Awarness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.[115] If a U.S. company adheres to these five principles, the FTC labels such compliance as a "fair information practice".[116] This form of compliance amounts to the "adequate" protection standard as defined by the Directive.

During privacy disputes under the Safe Harbor, a decision favoring an EU entity upon a showing that a U.S. company continually violates the "adequate" protection standard results in the case being brought under the FTC's jurisdiction.[117] Here, due process is afforded to the non-compliant U.S. company, but this company is immediately dropped from the Safe Harbor.[118] The consequence of such action is that the company

---

[111] *Id.*
[112] *Id.* at 6.
[113] *Id.*
[114] Blanke, *supra* note 7, at 70 (quoting Federal Trade Commission, *Privacy Online: A Report to Congress*, *available* at <http://www.ftc.gov/reports/privacy3/fairinfo.htm#FairInformationPracticePrinciples> (last visited March 30, 2003)).
[115] *Id.*
[116] *Id.*
[117] Ruth Hill Bro, *Privacy and Data Protection in the Business-to-Business Context*, 650 P.L.I./Pat 321, 328 (2001).
[118] *Id.*

puts itself into disrepute with the FTC, DOC, and EU entities. This puts a company at a disadvantage in terms of collecting personal data securely from EU sources. If an EU party learns of a company's failure to meet the "adequate" protection standard because it is dropped from the Safe Harbor, any correspondence made by this company may be blocked by an appropriate DPA. Thus, the ability to conduct online commerce with EU parties affects the business prospects of any non-compliant U.S. company doing business in the EU.

A similarity exists between the EU and the U.S. in terms of the structural arrangement of privacy authorities. Under Article 29 of the Directive, an advisory group known as the "Working Party" oversees the protection of consumers' personal data with regard to online commercial activities.[119] The Working Party ensures uniform privacy compliance in each EU member state, and is required by the EU Commission to submit annual reports regarding the status of personal data protections.[120]

The analogous U.S. enforcement body for privacy compliance is the FTC. Like the Working Party, the FTC submits annual reports to legislative bodies on privacy protection standards.[121] Many of the FTC's findings relate to consumer privacy issues.[122] For instance, a 2002 FTC Report reveals that up to $18 billion is lost in online retail due to data privacy concerns expressed by American consumers.[123] Such findings are enough to compel Congress to introduce legislation that safeguards personal data of American

---

[119] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, *The Protection of Individuals with Regard to the Processing of Personal Data and on the free movement of such Data, available at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 30, 2003).
[120] *Id.*
[121] FTC Report, *supra* note 51, at 1.
[122] *Id.* at 2.
[123] *Id.*

consumers. The FTC thus demonstrates how its monitoring of compliance standards within the U.S. helps prod legislative changes to the existing privacy regime.

(D) CONTRIBUTING TO COMPREHENSIVENESS: THE DEPARTMENT OF COMMERCE

The DOC is a key federal agency in helping the FTC regulate online privacy in the U.S. The DOC's commitment to ensuring "adequate" privacy protection is amply illustrated in a formal letter sent to the EU in 1999: "We will encourage U.S. organizations to enter the safe harbor as soon as possible to enhance privacy protection and because participation in the safe harbor provides greater certainty that data flows will continue without interruption."[124] Fifteen frequently asked questions (FAQs) are available on the DOC Safe Harbor website for companies interested in learning about all aspects of the Safe Harbor.[125]

The Safe Harbor website also includes a Safe Harbor Workbook, documents, public comments, and a Compliance Checklist for EU entities to review.[126] Like the FTC website for the "Dewie" initiative, the Safe Harbor website contains a link geared specifically for privacy statements.[127] The DOC also maintains a Safe Harbor list ("List"), which displays only those U.S. companies voluntarily participating in the Safe Harbor.[128] The List helps EU entities involved in online transactions with U.S.

---

[124] DOC website, *supra* note 45, *Data Protection: Draft of Letter from the U.S. Department of Commerce to the European Commission Services*, *available at* <http://www.ita.doc.gov/td/ecom/RedlinedUSLettertoEU.html> (last visited March 30, 2003).
[125] DOC website, *Safe Harbor Overview*, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited April 1, 2003).
[126] DOC website, *Safe Harbor Overview*, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 30, 2003).
[127] *Id.*
[128] DOC website, *The Safe Harbor List*, *available at* <http://www.ita.doc.gov/td/ecom/FRN2.htm> (last visited March 30, 2003).

companies to ascertain whether U.S. companies are complying with "adequate" privacy protections.

Both the FTC and DOC illustrate the commitment made by U.S. federal agencies in implementing the Safe Harbor. Working in a coordinated fashion to monitor "adequate" privacy protections within a traditionally sectoral regime, these two agencies are shaping U.S. privacy law to resemble EU comprehensive standards. This has much to do with the realization that maintaining data transfers between U.S. and EU entities is essential in preserving strong trade links. But aside from federal agencies changing existing privacy standards, States are also making great strides in contributing towards a more comprehensive privacy regime.

(E) CONTRIBUTING TO COMPREHENSIVENESS: MINNESOTA AND VERMONT

Individual states are moving toward comprehensiveness by expanding privacy protections for personal data provided by state residents during online commercial transactions. However, this trend is not entirely equivalent to the EU definition of comprehensiveness. This is because all industries handling personal data within States still self-regulate without being subject to an overarching regime. Instead, there are stricter "adequate" standards being introduced. Nonetheless, this trend suggests that States are moving towards some form of comprehensiveness.

Minnesota's adoption of the *Internet Consumer Privacy Act* ("ICPA") in May 2002 is a state initiative safeguarding the personal data of Minnesota consumers.[129] Labeled as Chapter 395, the ICPA is the first law among the States requiring online

[129] Memo from Dorsey & Whitney LLP, *Minnesota Enacts New Internet Consumer Privacy Law, available at* <http://www.dorseylaw.com/updates/cams/20020522.asp> (last visited March 30, 2003).

service providers to disclose their own information practices when receiving personal data from any Minnesota consumer.[130] The ICPA also prohibits the use of "false or misleading" e-mail messages whereby a provider uses a consumer's domain name without permission.[131] Damages may be awarded in the amount of $25 for each e-mail, or $35,000 per day for a violation of the "false and misleading" provision.[132]

Article 1 of the ICPA provides that a Minnesota consumer is entitled to $500 or actual damages for a violation of Minnesota's privacy laws.[133] The ICPA also requires the initiator of an e-mail message to have a toll-free phone number or return e-mail address to give consumers a choice on whether to receive future e-mails.[134] This requirement echoes the FTC Act's 'fair information practice' of providing relevant contact information.[135] The requirement also reflects the Safe Harbor "opt-out" option under the "Choice" Principle.[136]

Since March 1, 2003, the ICPA requires any online service provider soliciting business from Minnesota consumers to request direct authorization from the consumer to receive personal data.[137] Moreover, the online service provider must explicitly mark e-mail messages with "ADV" to give notice to the consumer that the provider intends to use its personal data with "adequate" privacy standards.[138] This requirement parallels the

---

[130] *Id.*
[131] *Id.*
[132] Minn. H. 395, 2002 Reg. Sess. (May 23, 2002), *House Research Act Summary*, *available at* <http://www.house.leg.state.mn.us/hrd/as/82/as395.html> (last visited March 30, 2003).
[133] *Id.*
[134] *Id.*
[135] Blanke, *supra* note 7, at 70 (quoting Federal Trade Commission, *Self-Regulation and Privacy On-Line: A Report to Congress* (1999), *available at* <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (last visited March 30, 2003).
[136] DOC website, *supra* note 45, *available at* <http://www.export.gov/safeharbor/sh_overview.html> (last visited March 30, 2003).
[137] *Id.*
[138] *Id.*

online privacy seal programs of TRUSTe and BBBOnline that require privacy seals on the website as evidence of meeting "adequate" privacy protection standards.

The ICPA is significant in that privacy protections espoused by federal standards are being reinforced under state law. The ICPA also reflects the growing concern expressed by American consumers over personal data protections. As the ICPA's legislative history suggests, Minnesota enacted privacy protections in response to concerns addressed by state residents over personal data collection practices of companies.[139] The Minnesota legislation thus demonstrates how a State favors newer and tougher measures to protect personal data used in online commercial transactions.

Like the Directive and the Safe Harbor's principle of "Choice", Vermont's privacy law in the health sector emphasizes "opt-in" measures for the consumer. Specifically, Vermont's "opt-in" privacy law affords protection of personal health care data of Vermont residents.[140] The "opt-in" law gives Vermont consumers the power to consent when disclosing personal data to relevant health authorities.[141] Moreover, Vermont consumers are required to "opt-in" when disclosing information to third parties, such as marketers.[142] Any party willfully disclosing personal health care data without the consumer's consent will face civil penalties of no greater than $10,000.[143]

Although Vermont's "opt-in" law is sectoral with respect to health care data protections, the law incorporates fundamental principles espoused in the Directive and

---

[139] Minnesota Consumer Alliance, *Issues – Privacy*, *available at* <http://www.mnconsumeralliance.org/issues_privacy.htm> (last visited March 30, 2003).
[140] Computer World, *New Vermont 'Opt-In' Privacy Law Faces Legal Challenge*, *available at* <http://www.computerworld.com/databasetopics/data/story/0,10801,68104,00.html> (February 7, 2002) (last visited March 28, 2003).
[141] *Id.*
[142] *Id.*
[143] Vt. H. 416, 66th Biennial Sess. (Jan. 3, 2001), *Privacy of Health Care Information*, *available at* <http://www.leg.state.vt.us/DOCS/2002/BILLS/INTRO/H-416.HTM> (last visited April 1, 2003).

the Safe Harbor. These principles relate to greater transparency on the part of the online provider. Much like the Directive and the Safe Harbor, § 9471(a)(4) of the Vermont privacy law requires: "Identification of individuals who are authorized to disclose health care information."[144] That is, any party receiving sensitive personal data from Vermont consumers is required to clearly identify itself for accountability purposes.

State legislatures are thus introducing more effective privacy controls over the content and use of personal data for state residents. Upon a review of the Minnesota and Vermont initiatives, specific elements of privacy protections found in the Directive and Safe Harbor are finding its way into state privacy laws. For instance, the Principle of "Choice" affords greater control over the content of personal data used in online transactions for consumers in both Minnesota and Vermont. But this trend in providing consumers with the power to regulate personal data within States is in response to a national concern expressed by American consumers over personal data protections.

In a wider sense, this trend suggests that individual states are equal to the task in adopting more comprehensive privacy laws much like the federal government. As states launch programs designed to increase uniformity in the realm of privacy, a growing number of U.S. businesses are being encouraged to back such initiatives. A report by the U.S. Senate Committee on Commerce, Science, and Transportation illustrates this point: "As momentum grows in the State legislatures and agencies across America to regulate privacy, some companies that previously opposed Federal legislation . . . now support a uniform standard that clearly preempts these various, inconsistent State laws."[145]

---

[144] *Id.*

[145] Online Personal Privacy Act, *Report of the Committee on Commerce, Science, and Transportation on Sen. 2201*, 107th Cong., 2nd Sess. (Aug. 1, 2002).

Although these State privacy laws may be inconsistent in nature, each industry is adopting similar privacy standards that may eventually coalesce to establish an overarching regime. Even if an overarching regime does not materialize, there may be enough uniformity in privacy standards within each industry that closely resembles comprehensiveness.

VI. GLOBAL TREND TOWARDS A COMPREHENSIVE PRIVACY REGIME

Many nations are adopting comprehensive privacy laws that reflect the principles of the Directive and Safe Harbor. For instance, Hong Kong introduced the Personal Data Privacy Ordinance ("Ordinance") on January 30, 2001.[146] The Ordinance regulates telecommunication services in direct marketing situations.[147] Overlooking the Ordinance, the Hong Kong Productivity Council (under the authority of a Privacy Commissioner) refers to specific criteria in determining how personal data should be transferred from the Council to outside parties.[148] Enforcement of privacy violations provides 'data subjects' with rights to correct inaccurate personal data.[149] Such rights bear a striking resemblance to the Principle of "Access" in that it provides consumers with an opportunity to access and correct any relevant personal data that could be misused by outside parties. Like the Directive and to some extent the Safe Harbor, the Ordinance involves tight government controls on the transfer of personal data.

---

[146] Office of the Privacy Commissioner for Personal Data, Hong Kong, *The Ordinance*, *available at* <http://www.pco.org.hk/english/ordinance/ordfull.html> (last visited March 28, 2003).
[147] *Id.*
[148] *Id.*
[149] *Id.*

In 2000, Canada introduced the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[150] PIPEDA involves a three-stage implementation process: (1) on January 1, 2001, personal data of clients and employees are protected in federally regulated private industries such as airlines, broadcasting, and banking; (2) on January 1, 2002, personal health data is protected; and (3) on January 1, 2004, PIPEDA standards will be binding on all Canadian provinces that "collect, uses or discloses" personal data in the course of commercial activities, whether or not the organization is federally regulated or not.[151] The first stage imposes PIPEDA standards on organizations that disclose personal data of Canadian citizens outside the country.[152] The federal government may exempt organizations from this implementation process if the commercial activity is within a province that adopts privacy legislation similar to that of the federal initiative.[153]

VII. CONCLUSION

Comprehensiveness is defined as a broad scheme that enforces strict "adequate" standards for personal data handled by all industries under an overarching regime. Since the Directive's adoption, five factors are shaping U.S. privacy laws to become more comprehensive in nature. First, the Directive is influencing U.S. privacy law in terms of setting a precedent for enforcing stricter privacy standards. Second, the influence of the Safe Harbor is such that it acts as a substitute for comprehensiveness in the U.S. privacy

[150] Office of Privacy Commissioner of Canada, *The Personal Information Protection and Electronic Documents Act*, *available at* <http://www.privcom.gc.ca/legislation/02_06_01_e.asp> (last visited March 28, 2003).
[151] *Id.*
[152] *Id.*
[153] *Id.*

regime. With widespread differences in privacy laws between the U.S. and the EU, the Safe Harbor serves as a useful intermediate link because it merges EU comprehensive privacy standards with U.S. sectoral standards.

The third and fourth factors, respectively, relate to Congress's growing concern over personal data protection, and States' increasing recognition that similar protections should be afforded to its own residents. Specifically, Americans are growing wary of personal data protection from online providers. Such concerns are prompting Congress to adopt more comprehensive privacy legislation. Fifth, concern over billions of dollars worth of trade between the EU and the U.S. is forcing the U.S. to consider more comprehensiveness in streamlining commerce between the two entities.

Over time, these five factors will gather momentum in helping shape a comprehensive regime within a system traditionally accustomed to a sectoral approach. Even if the EU version of comprehensiveness does not materialize in the U.S., it can be argued that various industries in the U.S. are adopting privacy standards so similar to EU standards that some form of comprehensiveness is being incorporated into a sectoral-based regime. Nonetheless, with respect to U.S. privacy law, this type of regime acts as a benchmark from which interested parties and relevant authorities may curb misuse of online personal data. The advantage of a comprehensive privacy regime is that it ensures uniformity and certainty in protecting personal data for online commerce.