UIC John Marshall Journal of Information Technology & Privacy Law

Volume 18
Issue 4 *Journal of Computer & Information Law - Summer 2000*

Article 5

Summer 2000

Falling Into the Gap: The European Union's Data Protection Act and its Impact on U.S. Law and Commerce, 18 J. Marshall J. Computer & Info. L. 981 (2000)

Marie Clear

COMMENTS

FALLING INTO THE GAP: THE EUROPEAN UNION'S DATA PROTECTION ACT AND ITS IMPACT ON U.S. LAW AND COMMERCE

For generations, the United States ("U.S.") has enjoyed its status as one of the world's commercial economic leaders, and one of the biggest benefits in being king of that commercial hill is the luxury of setting the rules. Any country that wanted to change the way we wanted to play had better bring some compelling economic force to bear. And, while the U.S. has occasionally been convinced to give in, the major players and their respective powers have remained comfortably familiar and relatively unchanged for decades.

Suddenly, though, there is a brand new competitor in the game – one that parallels the U.S. in both size and economic force, and one that sets its own rules without minding much whether the U.S. wants to keep playing. The European Union ("E.U.") has been economically consolidating for some time, but the U.S. appeared to feel this new composite player was relatively benign. In the past few years, though, the E.U. has started asserting itself and setting rules. Until recently, the rules were limited to specific products and practices. This year, however, the E.U. changed the rules about *how* it would do business and, more significantly, how it would not.

The E.U.'s Data Protection Directive came into force early in 2000 and presented the U.S. with a huge dilemma. If the U.S. would not alter its law to provide a specific level of privacy protection for E.U. customers, then the U.S., quite simply, could not do business with those E.U. customers. They presented the U.S. with an economic dilemma it simply cannot ignore any longer – one that may force the U.S. to close the privacy gap between its status quo policy of commercial data freedom and the E.U.'s pro-consumer privacy protections. This comment explores the history, the problems, and the possible solutions the U.S. might employ to avoid being disqualified from playing in the European arena.

I. INTRODUCTION

Each year, the European Union ("E.U.") moves closer to becoming the "United States of Europe" that Winston Churchill envisioned as early as 1946.[1] Initially, the relationship between the fifteen Member States[2] primarily promoted trading convenience.[3] Today, however, the Union has moved well beyond those administrative inter-European trade issues and is quickly creating a substantial body of unified law.[4] Even though each European country retained its individual legislature, every Member State is nonetheless subject to the recommendations, directives and regulations that are generated by the Union bodies, whether the laws are created by the E.U. as an organization or by the individual Member States under the Union's supervision.[5]

The structure of the E.U. bodies and their interaction is a complex weave of organizations, such as commissions, associations, councils, and committees, that were created by an even more complex bundle of treaties and agreements.[6] However, regarding Union law, we can generally limit our focus to three bodies: the European Commission, the European Council of Ministers, and the European Court of Justice.[7] The European Council of Ministers enact the policies and legislation recommended by the European Commission.[8] Once enacted, the given Union law controls over any national Member State laws that not only conflict with, but

1. RALPH H. FOLSOM, EUROPEAN UNION LAW IN A NUTSHELL 1 (1999). Churchill spoke in the context of protecting Europe from new conflicts between old enemies given the resurgence of Germany's coal and steel industries – necessary industries in mounting a war effort. *Id.* His focus, in this case, was on building a relationship between Germany and France, with the United Kingdom acting not as a participant, but as a patron of the partnership. *Id.*

2. *See* Ardan Folwaij, *European Union Info Page* (visited Oct. 3, 1999) <http://www.geocities.com/CapitolHill/Senate/6217>. The Member States are Austria, Belgium, Denmark, Finland, France, Germany, Great Britain, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, and Sweden. *Id.*

3. *See* European Union, *The European Union: Profile of the EU* (visited Oct. 3, 1999) <http:// www.eurunion.org/profile/index.htm> [hereinafter *Profile of the EU*]. Shortly after World War II, six European countries cooperated to form the European Coal and Steel Community. *Id.* Although a common market catering to coal and steel interests may not appear a natural first step in developing a comprehensive supranational government, the European desire to avoid the possibility of another war between European states prompted the coalition. *Id.* Common control of the war industries coupled with borderless markets created just the sort of economic interdependence that would help deter conflicts. *Id.*

4. *See* FOLSOM, *supra* note 1, at 31.

5. *Id.*

6. *See, e.g., id.*; *see also* KAREN V. KOLE & ANTHONY D'AMATO, EUROPEAN UNION LAW ANTHOLOGY (1998).

7. *See* Towson State University, Department of Political Science, *Organization and Institutions* (visited Sept. 28, 1999) <http://saber.towson.edu/polsci/ppp/sp97/eu/INSTITU.HTM>.

8. *See Profile of the EU*, *supra* note 3.

even those that merely interfere with, the E.U.'s legislation.[9] Should anyone find themselves at odds with E.U. rules, the European Court of Justice is the judicial body that interprets and applies the law.[10] The final verdict of the thirteen Court justices takes precedence over the Member State courts.[11]

The E.U., in an effort to standardize rules between participating nations and strengthen protections regarding technology, generated a number of recommendations that directly addressed technology-related issues.[12] Many are benign in that they simply standardize the rules of law or business practices already in place in many European countries.[13] The revised Data Protection Act, however, which has already been enacted by nine of the member states,[14] specifically addresses the issue of international information security, and this has presented a serious threat to the economic relationship between the United States ("U.S.") and the E.U.[15] The original law, the 1984 Data Protection Act, was de-

9. *See* KOLE & D'AMATO, *supra* note 6, at 61.

10. *See Organization and Institutions, supra* note 7.

11. *See* KOLE & D'AMATO, *supra* note 6, at 18.

12. *See, e.g.,* EUR. PARL. DOC. (OJ L 24) 1 (LEXIS Jan. 30, 1998) (mandating telecommunications privacy rules to protect consumers' privacy in areas such as communications, billing, and subscriber information); EUR. PARL. DOC. (OJ L 040) 1 (LEXIS Feb. 13, 1999) (amending regulations for airline and railway computer reservation systems, ensuring, amongst other things, free consumer access to personal data, appropriate privacy measures, and audit requirements that must be in keeping with the Data Protection Directive); EUR. PARL. DOC. (OJ L 203) 9 (LEXIS Aug. 3, 1999) (adopting measures to ensure that electronic data networks linking European Community organizations and Member State administrations are cross-compatible, that security and quality assurance practices are standardized, and so on).

13. *See* John Travers, *Case Study, Dublin Ireland: The Role of Information Technology in Attracting Foreign Investment, Creating Industrial Zones and Developing Human Resources, Address Before the World Competitive Cities Congress at the World Bank in Washington, D.C.* (visited Aug. 28, 2000) <http://www.forfas.ie/report/washington.htm>. Travers delivered his speech May 19-21, 1999. *Id.*

14. *See* European Union, *Data Protection: Commission Takes Five Member States to Court* (visited May 13, 1999) <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/2k-10.htm>. The remaining countries – those that have not enacted the data protection law – are being sued before the European Court of Justice for failing to implement the protection measures before the deadline established by the Data Protection Directive. *Id.* The countries being hauled before the courts for noncompliance are Denmark, Germany, France, Ireland, Luxembourg, and the Netherlands. *Id.* Clearly, the E.U. is painfully serious about the importance of implementing and enforcing these data protection measures.

15. *See* Karlin Lillington, *Data Protection Law to be Delayed until Autumn*, IRISH TIMES, July 19, 1999, *available in* 1999 WL 21894481.

> The directive is of particular concern to businesses because, if implemented as it stands, it could bring to a standstill the operations of the many European-based companies that exchange data with U.S.-based companies. Irish companies which do 'back office' processing of data for U.S. companies, are branches of U.S. multinationals, or operate international telecentres could all be affected.

signed to help European citizens control the use and distribution of their personal data.[16] Since then, the European Commission recommended strengthening the Act[17] by adopting the Data Protection Directive.[18] The Act and Directive were formally joined, amended, and brought forth as the revised Data Protection Act[19] in October, 1998, and Member States were to comply by early 2000.[20] Since its enactment, U.S. and E.U. officials have been negotiating extensively to find some way for the U.S. to satisfy the Act's strict data protection requirements without having to adopt the measure outright.[21]

In order to explore the potential impact of these E.U. data privacy rules on U.S. law and commerce, this Comment reviews the U.S. Constitutional, legislative, common law, and commercial self-policing protections that are currently in place in the U.S. as compared to the current state of European data privacy protections. After analyzing the relative effectiveness of U.S. efforts to develop and manage data protections, the

---

Id. at 1.

The time is coming fast, even as the U.S. and E.U. negotiators continue to try to resolve the problem, as seven E.U. Member States have already adopted the directive. *Id.* Time is growing short for the U.S. to make a final resolution if individual countries are beginning to adapt their commercial law to accommodate the Directive as it stands. *Id.*

16. *See Legal and Financial: Firms Face Huge Paper Chase over New Data Protection Rules*, BIRMINGHAM POST, July 2, 1999, *available in* 1999 WL 20262069. The original Act focused on allowing people to control any electronic personal data, or in other words, personal data that could be "processed." *Id.* The new Directive includes paper-based records in some circumstances, which means that in order to comply with the amended Act, companies will have to look through and account for all of the data on all of the paper in their possession. *Id.* Instead of individuals controlling their own personal data, they will control, to a great extent, the productivity and liability of the companies with paper-based documentation that happens to be protected by the Act. *Id.*

17. *See* David Reed, *European Legislation: Au Fait with EC Laws or in Need of Directives?*, PRECISION MARKETING, Apr. 20, 1998, *available in* 1998 WL 8680332. The first version of the Directive was so strong as to be considered "draconian" by some in the marketing industry. *Id.* Fortunately, the process of revision and amendment over the past years has had a moderating effect that has made the Directive a workable rule, though commercial interests remain watchful. *Id.*

18. *See* Data Protection Section, U.K. Home Office, *Consultation Paper on the EC Data Protection Directive (95/46/EC)* (1996) <http:// www.homeoffice.gov.uk/ccpd/ dataprot.htm>.

19. *See* Parliament and Council Directive 95/46/EC of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Annex, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

20. *See* Geoff Winestock ET AL., *A Special Background Report On European Union Business and Politics*, WALL ST. J. EUR., Sept. 23, 1999, *available in* 1999 WL-WSJE 27639716. *See also* European Union, *Directive on Personal Data Protection Enters into Effect*, (visited May 13, 2000) <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/925.htm>.

21. *See* Elizabeth de Bony, *EU and U.S. Extend Data Privacy Negotiations* (Dec. 20, 1999) <http://www.computerworld.com/home/news.nsf/all/9912201privacy>.

Comment makes general recommendations suggesting a course of action for achieving consistent and comprehensive data protection rights into the next decade. The U.S. must be more pro-active and develop a stronger set of data protection rules that are both consistent and easy to apply. What kind of message will it send to U.S. citizens if European consumer data is protected, while our own personal information remains commercial fodder?

II. BACKGROUND

The European data protection rules are designed to protect individuals from having their personal information spread indiscriminately amongst commercial, governmental, or private information miners.[22] If those "data gatherers" choose to transfer someone's personal data to another entity, they first must prove the person gave them permission to use the data that way – whatever the data and whatever the use.[23] Without permission to use the personal data, companies can only use the information for its original purpose.[24] This use restriction, however, is only one of the principles contained in the Act.[25] Companies must go even further by developing pro-active measures, such as methods to ensure the data is not gathered fraudulently, an offense under the Act in order to comply.[26] The key principles enumerated by the original 1984 Data Protection Act are that data must be legally obtained; used only for the purposes described in the registration; relevant to that purpose and not excessive; accurate and up-to-date; held only as long as necessary; protected by proper security; and accessible by the individual to whom the data refers so that he can correct or delete it if appropriate.[27]

---

22. *See Consultation Paper on the EC Data Protection Directive*, *supra* note 18. Both the Act and the Directive define "personal" data quite broadly, as being "any information relating to an identified or identifiable individual." *Id.* The Act limits its definition of "identifiable" to mean that the individual is identifiable only if the data user can identify the individual from the information. *Id.* The Directive, however, takes a broader view and holds that an individual is identifiable if *anyone* has data that allows the individual to be identified. *Id.*

23. *See Private, Keep Out*, PC DEALER, July 21, 1999, *available in* 1999 WL 7760380.

24. *See id.*

25. *See Consultation Paper on the EC Data Protection Directive*, *supra* note 18.

26. *See Private, Keep Out*, *supra* note 23.

27. *See* Data Protection Directive, *supra* note 19. On principles relating to data quality, the Directive provides:

> 1. Member States shall provide that personal data must be:
> (a) processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

A. THE DISPUTE

In keeping with the goals of protection and control, one of the Data Protection Directive's mandates is that no one may transfer personal data outside the E.U. to "countries that do not provide an 'adequate' level of privacy protection."[28] Unfortunately, this is one of the key points threatening the flow of trade between the U.S. and the E.U.[29] The im-

---

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Id.

28. *See* Data Protection Directive, *supra* note 19. On matters regarding the transfer of personal data to third countries, the Directive provides:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

Id.

29. *See* The United States Mission to the European Union, *USIA Foreign Press Center Briefing Topics: U.S.-EU Trade Relations, Internet Commerce and Privacy Issues, Briefer: David Aaron, Under Secretary of Commerce for Trade, Washington* (Jan. 22, 1999) <http://www.useu.be/archive/aaron122.html> [hereinafter *Aaron: USIA Foreign Press Center Briefing*].

pact could be enormous if the two trading partners cannot negotiate a compromise.[30] This issue of requiring protection after data is transferred is a fundamental problem for the U.S. on a number of different levels,[31] since it requires any non-Union recipients of Union personal data to abide by the terms of the Act.[32] The earlier Act had no such burden for any country outside the Member States, which had formerly kept the 1984 Act from impacting the U.S.[33]

Needless to say, the U.S. business community is not inclined to simply adopt the E.U.'s new Data Protection Act outright, given that the Act comes with significant reporting responsibilities.[34] U.S. companies specifically object to two elements of the Act: the disclosure requirement allowing an individual to access all of his own personal data and the technical difficulties involved in implementing the protections.[35] The most serious issue from the E.U.'s perspective is in allowing the U.S. to receive personal data regarding their citizens, without a suitable U.S. authority to turn to if someone breaks the rules.[36]

While it is certain the U.S. and the E.U. will come to some agreement to keep trade flowing, it is also certain that the U.S. will technically violate the Data Protection Act as it stands regardless of what is done to comply.[37] For example, the personal information in e-mail and message packet routing[38] is "personal information."[39] The potential impact on electronic communications is mind-boggling considering that every U.S. Internet server may be unintentionally exposed to the re-

30. *See id.* "If this problem isn't solved, if data gets interrupted, this isn't just going to harm American companies or the United States." *Id.* "This is going to have a very adverse impact on the operation of the economies on both sides of the Atlantic and, indeed, could be a very serious blow." *Id.* "So the stakes are very high." *Id.*

31. *See* Lillington, *supra* note 15.

32. *See id.*

33. *Cf. Consultation Paper on the EC Data Protection Directive*, *supra* note 18 with the Data Protection Act 1984.

34. *See* DowJones.com, Dow Jones Business News, *U.S. Official Optimistic Data-Privacy Talks With E.U. Will Bear Fruit* (Sept. 17, 1999) <http://dowjones.wsj.com/p/main.html> (resulting from search of "'Data Privacy' and 'bear fruit'" in Business Search field).

35. *See* Lillington, *supra* note 15.

36. *See U.S. Official Optimistic Data-Privacy Talks With E.U. Will Bear Fruit*, *supra* note 34.

37. *See* Annie Gurton, *Walk on the Wild Side. Are You Breaking the Law?*, ACCT., June 7, 1999, *available in* 1999 WL 14997366.

38. *See id.* E-mail headers and routing information are dense and humanly illegible compactions of gibberish that are technically decipherable nonetheless. *Id.* The Act allows that if reasonable effort can be expended and the information can be deciphered to identify a living individual, then the information is covered by the Act and has to be protected as such. *Id.*

39. *See id.*

quirements of the Act.[40]

Given that the E.U. has become a significant trading partner with the U.S. with strong import and export figures for goods and services, the dispute is a serious one.[41] While Internet commerce transactions in the E.U. are significantly lagging behind U.S. consumer purchases,[42] those statistics are expected to rise quickly,[43] making E.U. Internet spending an even greater contributor to Union and U.S. trade. Before the E.U. became a single economic entity, no one European country had as crucial a trading relationship with the U.S. as does the unified E.U.[44] Combined into a single trading partner, the Union has the kind of trading power that makes it critical to find common ground.[45]

Although negotiations between the U.S. and the E.U. continue, the U.S. is staunchly against abiding by the currently proposed Act.[46] However, without agreeing to abide by the Act, the U.S. will not be able to receive any personal information from Union citizens, such as addresses,

---

40. E-mail, when it is being sent from one person to another, often takes a wildly circuitous route that works much like telephone switching stations. So, for example, in sending an e-mail from Chicago to New York, it may go via Denver. In the case of e-mails being sent between users in the E.U., it is possible that e-mails will inadvertently travel via a U.S. server on its route someplace else entirely. These are the variables introduced by computer technology that would not have been an issue ten years ago, but that have nonetheless complicated our lives and our trading relations in unexpected ways.

41. *See* BUREAU OF THE CENSUS, REPORT FT900 (CB-99-169), *Foreign Trade Division, FT900 - U.S. International Trade in Goods and Services* (July 1999) (visited Oct. 12, 1999) <http://www.census.gov/foreign-trade/Press-Release/current_press_release/exh14.txt>. As of July, 1999, the U.S. exports to the Union in July exceeded $11 billion, and the annual first half cumulative figure was nearly $89 billion. *Id.* July imports from the Union passed $17 billion, contributing to a six month import figure of more than $110 billion dollars worth of goods and services coming into the U.S. from the E.U. *Id.*

42. *See* Bob Tedeschi, *European Union Advances E-Commerce Policies*, N.Y. TIMES, Apr. 26, 1999 (visited Oct. 5, 1999) <http://www.nytimes.com> (resulting from search of Tedeschi and "European Union" in Search field). U.S. consumers spent $5 billion over the Internet in the 1998 Christmas holiday season alone, whereas E.U. consumers used the Internet to purchase only $650 million worth of goods throughout the entire year of 1998. *Id.*

43. *See id.*

44. *See* BUREAU OF THE CENSUS, *supra* note 41.

45. *See* The United States Mission to the European Union, *U.S. House of Rep. Comm. on International Relations* <http://www.useu.be/ISSUES/aaron0617.html> [hereinafter *Aaron: U.S. House of Rep. Comm. on International Relations*]. Regarding the economic relationship between the U.S. and the E.U., Mr. Aaron stated, "[t]he United States and the E.U. share the largest two-way trade and investment relationship in the world." *Id.* This is the reason that regardless of the ideological differences, the two organizations will come to a workable agreement regarding the Act. *Id.* However, the issue will hopefully be decided on the legal merits, rather than a cat-and-mouse economic chess match, given that both the U.S. and E.U. could benefit from a balanced compromise on this issue. *Id.*

46. *See* Lillington, *supra* note 15 (describing the dispute as "the subject of a major row between the US and the EU"). *Id.*

demographics, credit reports, and most ominously, credit card information.[47] The U.S. consumer and Internet import-export market may potentially shut down, at least where the E.U. is involved. According to David Aaron, U.S. Commerce Department Under-Secretary, the losses will be astronomical if the U.S. and E.U. cannot agree on some protection terms.[48] Interrupting commercial data between the U.S. and the E.U. means interrupting the cash flow between the two, which jeopardizes not only trillions of dollars in trade, but the entire international e-commerce industry.[49]

B. NEW MARKET

The stakes in personal data have risen ever since direct marketing graduated from random newspaper inserts and sidewalk leaflets handed out on street corners to a science all its own.[50] Technology has transformed that industry[51] to the point that almost anyone can find out any-

47. *See id.* "For consumers, the Act could prevent basic electronic commerce transactions because, without a resolution on data-handling issues, US companies could not accept credit card details from Europeans." *Id.*

48. *See Aaron: U.S. House of Rep. Comm. on International Relations, supra* note 45.

49. *See id.* "Blockage of data could threaten billions if not trillions of dollars or euros in international trade and investment . . . . Beyond that, the very future of the vastly promising electronic commerce marketplace may well hang on whether we can find ways to bridge our final differences." *Id.* Although it appears at first glance that the U.S. is alone in its frustration over elements of the Act, some European businesses are likewise at a loss. *Id.* Since the enactment of the Directive has taken so long and passed through so many iterations, some European businesses are hesitant to go ahead with computer system development or installs until the Directive is finalized. *Id.* The uncertainty about how personal data should now be handled likewise brings anxiety to the business persons attempting to abide by the spirit of the upcoming law. *Id.*

50. *See* Reed, *supra* note 17. One of the primary interests of the Data Protection Directive was originally to combat direct mail intrusions into the personal information of potential recipients. *Id.* Ironically, the Directive included a restriction on the practice of "profiling," which uses market research data coupled with demographic data to define the sort of person (by age or interests, for example) the marketer wants to specifically target. *Id.* However, had the profiling ban remained in the newer version of the Directive, direct mailings would have to increase exponentially and the marketing industry would have to return to relying on the blanket distribution techniques that are epitomized in newspaper inserts and leaflets. *Id.* As the legal and legislative affairs director of the DMA (UK) put it, "[t]o get to 10,000 target customers, you would have had to mail the whole country." *Id.* "That argument was very effective [in fighting profiling limits]." *Id.*

51. *See* The United States Mission to the European Union, *Remarks of Ambassador David L. Aaron, Under Secretary of Commerce for International Trade before the French and American Business Community American Chamber of Commerce Conference Center, Paris* (Jan. 1999) <http://www.useu.be/ISSUES/aaron126.html> [hereinafter *Aaron: French and American Business Community*].

thing about anyone else.[52] Businesses, as most everyone knows, are particularly efficient at finding their way into our homes by way of phone calls, e-mails, Internet ads, direct mailings, and a mass of other "directed" ways.[53] While we, as plagued consumers, may be unhappy about having our personal space and private information intruded on,[54] the issue is clearly a double-edged sword.[55] We as citizens, much less as consumers, are acutely interested in the health of the U.S. economy and cannot afford to underestimate the economic bounty offered by marketing and the Internet.[56] Likewise, we cannot dismiss the bounty that E.U. trade offers.[57]

Given the impact that the amended Act may have on foreign trade, there are significant legal issues facing both the U.S. and Europe. Earlier Directive drafts, while well-intentioned attempts to protect consumers in an increasingly intrusive environment, were pro-consumer to the point of being anti-commerce.[58] On the other hand, the U.S. is painfully slow to protect consumers from flagrant commercial intrusions and abuses.[59] Although there have been other trade conflicts between the

---

52. *See Private, Keep Out*, *supra* note 23. "Information," says Chris Rowsell of *Which?* magazine, "is becoming a currency – in some circumstances you are effectively paying for a service with your demographic information." *Id.*

53. *See* The Direct Marketing Association, *Direct Marketing to Business Conference Highlights* (Sept. 1999) (visited Oct. 5, 1999) <http://www.the-dma.org/topframe/index4.html>.

54. *See* Sarbanes, 145 CONG. REC. S554-01, S615 (West 1999) (statement of Sen. Sarbanes) "While cross-marketing can bring new and beneficial products to receptive consumers, it can also result in unwanted invasions of personal privacy without customers' knowledge." *Id.* The Senator points out the irony in having Federal legislation to protect information regarding individual's video rental selections and choice of cable TV channels, but there is no law keeping financial institutions from selling or trading individual's most private financial details. *Id.*

55. *See Aaron: French and American Business Community*, *supra* note 51.

56. *See id.*

57. *See Aaron: U.S. House of Rep. Comm. on International Relations*, *supra* note 45. Unfortunately, it appears the two sides are not sufficiently fearful of losing the economic bounty, considering that it took the two lead negotiators until mid-1999 to simply agree on the principles of "privacy." *Id.*

58. *See* Reed, *supra* note 17. When the original version of the Directive was introduced, it included extremely harsh requirements that would severely restrain marketing. *Id.* Various interests, including marketing lobbies, lashed out against those restrictive elements of the Directive prompting members of the Commission to revisit not only the Directive, but to research the problems in their developmental process that resulted in a proposal that was so strongly opposed by commercial interests. *Id.* The result was the introduction of checks and balances such as outside consultations and a generally more receptive body of commissioners. *Id.*

59. *See* Ann Sayer, *Industry Promises ISP 'Trustmark' Protection Standard Aimed at Increasing Consumer Confidence*, NETWORK NEWS (EUR.), Sept. 22, 1999, *available in* 1999 WL 9136676. In the absence of governmental action, businesses are moving forward to develop industry standards regarding data protection designed to satisfy E.U. privacy con-

U.S. and E.U.,[60] those problems are generally limited to specific products.[61] If the flow of credit card information stops, however, the impact will be significantly more noticeable to the U.S. economy than past banana and beef battles.

While these data protection issues may be the most prominent focus of the current U.S.– E.U. negotiations, there are still other data privacy problems facing individuals, such as identity theft, credit card fraud, and countless new data misappropriations that are downright criminal.[62] These combined problems have heightened U.S. citizens' concerns and prompted individual pieces of legislation designed to protect against specific abuses.[63] Unfortunately, despite this legislation, there are still terribly wide gaps exposing U.S. citizens to both legitimate and illegitimate intrusions.[64] Indeed, the state of privacy, consumer protection, and technology law has simply not kept pace with technology itself, and it is pre-

---

cerns. *Id.* In September 1999, IT business leaders proposed a self-regulated business-to-consumer protection initiative called "trustmark" which affords consumers certain defined protections and rights when they conduct business over the internet. *Id.* Thomas Middelhoff, chairman and CEO of one of the participating companies, commented on the U.S. and E.U. dispute over the Data Protection Directive saying, "We can't always wait for governments to find solutions." *Id.*

60. *See* Warner Rose, *Barshefsky Cites Progress in U.S.-E.U. Trade Relations* (June 21, 1999) <http://www.useu.be/ISSUES/barsk0622.html>. Charlene Barshefsky, the U.S. Trade Representative in negotiations with the E.U. on conflicts such as the E.U. ban on beef treated with growth hormone, said that there are relatively few problems between the U.S. and E.U. considering the enormous volume of business that is transacted. *Id.* However, she acknowledged the importance of equitably resolving the conflicts that do exist, saying "these are irritants that over time are corrosive." *Id.*

61. *See* BUREAU OF THE CENSUS, *supra* note 41.

62. *See* Jake Kirchner, *Protect Your Digital Identity*, PC MAG., Sept. 21, 1999, *available in* WL ISSN 0888-8507. "In the past, someone trying to steal your identity would have to gain access to paper records by breaking into your home or car, sifting through your trash, or combing public directories." *Id.* "Now almost all the data is available to any computer linked to the Internet." *Id.*

63. *See, e.g.*, Sarbanes, 145 CONG. REC. S554-01, *supra* note 54 (introducing the Financial Information Privacy Act of 1999 that would protect the privacy of personal information possessed by financial institutions); *see also* Roberta Furger, *Get This #$?* Spam Outta Here!*, PC WORLD, Sept. 1, 1998 (describing the antispamming amendment designed to protect consumers from anonymous commercial e-mail and proposing to give consumers the right to opt-out of receiving advertisements and other commercial communications from the given individual or organization in the future); Margaret Mannix, *Don't Call Me Again or I'll Sue*, U.S. NEWS & WORLD REP., May 3, 1999 (describing the Telephone Consumer Protection Act of 1991 which protects consumers by requiring telephone solicitors to maintain no-call lists and providing sanctions for violations).

64. *See, e.g.*, Jason Catlett, *What Can Be Done About Junk E-Mail?*, USA TODAY, Nov. 26, 1998 (*available in* WL ISSN 0161-7389) (providing statistics on U.S. telemarketing call rates and junk mail rates as being 10 billion telemarketing calls received per year, and 70 billion pieces of direct mail received per year); *see also* Kirchner, *supra* note 62 (comparing 35,000 complaints of fraud reported to a credit information service in 1992 versus 500,000 cases reported in 1997 by the same service, with two-thirds involving identity theft).

cisely this surge in technology that is magnifying the problems.[65]

C. Absence Of Regulation

Privacy law and Constitutional protections are the twin elements comprising the root of the debate over personal data in the U.S.[66] It is important to appreciate exactly what the U.S. legal system considers a "right to privacy" and where that supposed right stems from.[67] Samuel Warren and Louis Brandeis ushered in the beginnings of U.S. privacy law with an eloquent law review article that chaffed primarily at the press' intrusion into "private" affairs.[68] Years after that article, William L. Prosser further defined the nebulous right in terms of four causes of action: "(1) appropriation of the defendant's name or likeness for commercial benefit; (2) unreasonable intrusion, or intentional interference with a plaintiff's interest in solitude or seclusion (either in his person or in his private affairs); (3) public disclosure of private facts; and (4) publicity which places the plaintiff in a false light."[69] He earned the right to be considered the father of U.S. privacy principles, and the article provided the root of modern privacy law.[70] However, muddy boundaries still separate clear cases of privacy violations from those that simply *feel* like privacy violations. Prosser's article was written in 1960,[71] so it is no surprise that the Supreme Court of the mid-1960's struggled to define

65. *See* Sarbanes, *supra* note 54, at S616. The Senator plainly states that commercial self-regulation in the absence of legislation has not worked where data protection is concerned and urges Congress to move to enact legislation – legislation that is well overdue – to properly protect individuals and their personal data from abuses. *Id.* Citing a 1998 survey, 88% of consumers feel their personal privacy is threatened, and 61% feel that laws do not adequately protect their privacy. *Id.*

66. *See* Pamela Samuelson, Book Review, 87 CAL. L. REV. 751, 758 (1999). Although Americans cherish certain rights as fundamental to citizenship, they do not generally consider data privacy to be among them. Americans are more likely to cherish the principles embodied in the First Amendment – which favors a free flow of information – as fundamental human rights (quoting Peter Swire at 153 (discussing Americans' nearly religious attitude toward First Amendment rights)).

67. *See* Ian C. Ballon & Keith M. Kupferschmid, *Intellectual Property Opportunities and Pitfalls in the Conduct of Electronic Commerce: Practicing Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series*, 563 PLI/Pat 9 at 140 (June 14-15, 1999).

68. *See* THOMAS MCCARTHY, RIGHTS OF PUBLICITY AND PRIVACY §1.3B (1992). There was some conjecture, that does not appear accurate in retrospect, that the famous article was the product of a very irritated father. *Id.* "Seventy years later, Prosser caustically observed that the right of privacy was 'a most marvelous tree to grow from the wedding of the daughter of Samuel D. Warren . . . This was the face that launched a thousand lawsuits.'" *Id.* "Prosser was referring to what he thought where the real life events which prompted Warren and Brandeis to write their article." *Id.*

69. *See* Ballon, *supra* note 67, at 144-45.

70. *See id.*

71. *See id.*

the precise Constitutional basis for the new protective right.[72] Since privacy is not explicitly expressed, much less defined, in the Constitution, the Court used the penumbra doctrine[73] to draw it out.[74]

The underlying issue with Data Protection Act is the very different perspectives the U.S. and E.U. have regarding individual rights, corporate freedoms, and legislation.[75] Finding a compromise that balances these sometimes competing needs is key to the continuing success of the U.S.–E.U. economic relationship.[76] E.U. legal trends regarding the sanctity of personal data are clearly defined in the mass of acts, directives, amendments, and the like that are currently being developed.[77] In the

72. *See, e.g.,* Griswold v. Connecticut, 381 U.S. 479 (1965). In this case, the Supreme Court was struggling to extend privacy protection to married couples regarding their use of contraceptives. *Id.* at 480. Clearly, the court did not want the state to be allowed pry into marital bedrooms to expose use of contraceptives, and so determined that a couple's right to privacy in such matters outweighed the state's need to know. *Id.* at 507. What was interesting, though, is how many places the justices had to look to find such a protection. *Id.* They invoked the First Amendment, regarding its extension to protect associations, to protect parents' choice of schools, or to study subjects or languages, the Fourteenth Amendment right to due process was implicated, the Third Amendment right of privacy in keeping soldiers out of your house in peace-time, the Fourth Amendment right of privacy against unreasonable search and seizure, the Fifth Amendment right of privacy implied in the self-incrimination clause, and the Ninth Amendment umbrella that keeps the Constitution from impinging on individual rights retained by the people, suggesting that if the privacy right resides somewhere else, the Constitution cannot be turned to impede it. *Id.* at 482-84. Indeed, some of those who disagreed in part or dissented pointed out the scattered sowing of implied rights and "penumbras" the Court had to strew over the Constitutional Amendments in apparent hope that some would take root. *Id.* at 528. Fortunately, it is clear today, some did.

73. *See* BLACK'S LAW DICTIONARY 1135 (6th ed. 1990). "The implied powers of the federal government predicated on the Necessary and Proper Clause of the U.S. CONST. ART. I, §8, cl. 18, permits one implied power to be engrafted on another implied power." (quoting Kohl v. U.S., 91 U.S. 367, 23 L.Ed. 449).

74. *See, e.g., Griswold*, 381 U.S. 479.

75. *See* Tedeschi, *supra* note 42. Europeans and Americans are somewhat culturally polarized on these issues. *Id.* Europeans tend to be suspicious of big business and are more likely than the U.S. to impose regulations or legislation to protect individual rights, whereas the U.S. is focused more on economics and therefore tends not to favor legislation that would restrict business. *Id.*

76. *See id.* Despite the differences between the U.S. and E.U. on matters of personal data, there is some feeling that as the E.U. becomes more involved in the business of Internet commerce – at the moment Europe is significantly lagging behind the U.S. in e-commerce – the over-protective data protection focus of Europe and the somewhat paranoid fear of legislation on the part of the U.S. will both moderate as Internet and data "best practices" come to the foreground. *Id.*

77. *See, e.g.*, EUR. PARL. DOC. (OJ L 24) 1 (LEXIS Jan. 30, 1998), *supra* note 12, at art. 4. This Directive is a comprehensive package of protections prompted by the technological advances in telecommunications and digital technology, such as cellular phone systems, video-on-demand, and interactive television. *Id.* These new technologies raise privacy issues for consumers in billing, usage, and regulatory arenas. *Id.* The Directive outlines

U.S., the key legal principle protecting personal information is the right to privacy articulated by Samuel Warren and Louis Brandeis in their *Harvard Law Review* article.[78] The question is whether fundamental U.S. legal theory, in the context of data privacy, is sufficiently parallel to the spirit of the Data Protection Act. If so, it is possible that strengthening existing U.S. privacy, consumer protection, or technology law will approach meeting the Act's requirements.[79] If U.S. law is so significantly divergent from the spirit of the Act that harmony is unlikely, the U.S. is faced with the uncomfortable choice between making striking legal changes or losing international trading partners as the rest of the world moves towards more protectionist policies.

III. ANALYSIS

A. CONSTITUTIONAL PRIVACY PROTECTIONS

The Supreme Court's definition of the right to privacy provides for an "expectation" test that makes it difficult to enjoy the protective powers of the Constitution. In applying the right to privacy, for example the right protecting citizens against unreasonable search and seizure, the U.S. Supreme Court examines "whether the person who claims the protection of the [Fourth] Amendment has a legitimate expectation of privacy in the invaded place."[80] The Court defined a two-pronged test required for this Fourth Amendment analysis: the person must have "manifested a subjective expectation of privacy"[81] and the expectation must be "one that society accepts as 'objectively reasonable.'"[82] How-

---

regulations regarding processing consumer data and protecting individual's privacy in the telecommunications sector in a manner that supplements the Data Privacy Directive by defining the actual communications between telecom customers, traffic and billing data, itemized billing, identification of calling line and connected line, cross-border services such as video-on-demand and interactive television, ISDN computer connections and digital cell phones, and the subscription information and billing data for customers. *Id.*

78. *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Warren and Brandeis focused much of their attention on the right to privacy as against nosy media and curious neighbors and none of it on commercial trade in personal data in the sense that we mean today. *Id.* Yet theirs is still the analysis that triggered the flowering of the right to privacy in the U.S. and the cornerstone of the body of law that built the U.S. privacy right. *Id.*

79. *See id.* at 193. Warren and Brandeis eloquently characterized the flexibility of U.S. law, writing, "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society." *Id.* As technology speeds forward, this flexibility may well be key to our being able to protect ourselves against the unforeseen forces that travel with technological developments.

80. *See* United States v. Hambrick, 55 F. Supp.2d 504, 506 (1999), citing Katz v. United States, 389 U.S. 347 (1967).

81. *See Hambrick*, 55 F. Supp.2d at 506 (citing California v. Greenwood, 486 U.S. 35, 39 (1988)).

82. *See id.* at 506.

ever, the moment a person discloses information to a third party, even in the context of his own home, this "expectation of privacy" dissolves.[83] In regard to Internet Service Providers ("ISPs"),[84] for instance, a person who turns over information directly to the company, such as billing information, is not protected by an expectation of privacy under the Fourth Amendment. However, when someone sends an e-mail over the ISP's network to someone else, the sender does retain a privacy expectation.[85] For example, when an America Online ("AOL") customer initially "volunteers" personal information in order to open her account, the data is not protected, but when she sends an e-mail via AOL to another individual, she does have a reasonable expectation of privacy. The irony, of course, is that the customer is required to disclose the billing information in order to get Internet access, and she would be faced with the same dichotomy regardless of which ISP was selected - AOL or any of a host of other Internet access providers. Furthermore, the customer undoubtedly expects the data to be used for billing purposes, yet the expectation of use or scope of use does not appear to play a role in defining whether or not the data is protected.[86] Once the disclosure is made, the data is "public."[87]

One manor in which this paradox of "voluntary" transmission of personal information can be resolved is to add in the element of consent on the customer's part. Before a customer is required to "volunteer" information for a specific purpose, such as to open an Internet account, there should be an obligation that the company clearly disclose additional uses

83. *See id.* (citing *Katz*, 389 U.S. at 353).

84. *See* internet.com, *ISP Glossary* (1999) (visited Nov. 27, 1999) <http://isp.webopedia.com/> (resulting from search for "ISP"). An Internet Service Provider (ISP) is any company or organization that allows outside users to connect to the Internet using the computer hardware owned by that company or organization. *Id.* The most common type of ISP is a commercial Internet access company such as America Online, CompuServe, or Prodigy. Once a user has an established account, he or she may set up their personal computers to dial into the company's server. *Id.* When the dial-in access is successfully connected, it is the ISP's computer hardware and network that connects to the Internet itself. *Id.* Customers can then "browse the Web," exchange e-mail, and enjoy all of the benefits of internet access without personally having to sustain the significant costs and overhead of establishing a direct connection to the Internet, which is generally made through a major hub such as a university or research laboratory. *Id.*

85. *See Hambrick*, 55 F. Supp.2d at 507. The court in this case explicitly states, however, it is not enough that the ISP can access the data. *Id.* In the example of e-mail sent from one person to another, by virtue of using the ISP's service, a copy of every e-mail sent over their network is saved on computers owned by the company. *Id.* It is therefore technically possible for the ISP to access any given e-mail and read the contents. *Id.* However, the language of this court decision, ". . .the Internet service provider's ability to access the data must not constitute a disclosure," plainly protects information sent via their network but intended for another recipient. *Id.*

86. *See id.*

87. *See id.*

of the data. Any potential customer who is not satisfied with the company's usage policy, can simply retain another provider with a more acceptable policy. A customer's disclosure would then be "voluntary" informed consent. The company's subsequent use is legitimized rather than allowing the company to continue capitalizing on an uninformed disclosure as is currently the situation. However, the current system continues to define an uninformed voluntary disclosure as having dissolved any privacy expectation.

The Supreme Court's two-pronged test – that a person must have a subjective expectation of privacy that society believes is objectively reasonable – is described as a "risk analysis" test.[88] It poses tremendously difficult challenges to courts where new technologies, particularly the Internet and computer networks, are concerned.[89] A key case, for example, involved credit card users who attempted to keep their credit card company from renting client lists and purchase information to other companies.[90] The court held that so long as personally identifiable individual financial information was not passed on to third-party companies, the cumulative lists of individual buying habits do not violate the customers' privacy, since the customers voluntarily used their cards.[91] This issue of voluntary disclosure, while better defined in traditional business transactions such as credit card use, may be an area where Internet privacy rights need heightened protection.[92] This dilemma boils down to whether the courts find that increasingly well-informed technology users are also increasingly aware of the risk of having their personal data intercepted when they use such technologies.[93] Can a technology – savvy

88. *See id.*

89. *See id.* at 508.

90. *See* Dwyer v. American Express Co., 273 Ill. App. 3d 742 (1995).

91. *See id.* The plaintiffs in the case also alleged a violation of the Illinois Consumer Fraud Act (815 ILL. COMP. STAT. 505/10a(a) (West 1992), then Ill. Rev. Stat. 1991, ch. 121 1/2, par. 270a). *Id.* at 749. The court found that "the undisclosed practices of defendants are material and deceptive," that "defendants intended for plaintiff's to rely on the nondisclosure of their practice," and that the third and final element, that the deception occurred in the course of a commercial transaction, was not at issue in the case. *Id.* at 750. The plaintiffs, therefore, were successful in addressing all three of the required elements defined under the act. *Id.* However, the introductory phrase to this act states that it covers anyone who "suffers damage" because of a violation. *Id.* Regarding this, the court found that the plaintiffs suffered no actual damage by the disclosure, whether financial or from mental anguish, apart from a possible spate of unwanted mail. *Id.* It therefore decided that the American Express company was not liable for the disclosures. *Id.* at 751.

92. *See* Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 No. 5 COMPUTER LAW. 7 at 10 (May, 1999).

93. *See, e.g., Hambrick*, 55 F. Supp.2d 504 (1999) (holding that an Internet user had no expectation of privacy where his personal information regarding his screen name, which is an alias Internet users may employ to avoid disclosing their identities on-line, name, address, and so on, were not protected by an expectation of privacy on the user's part); *see also*

user really believe that his information is difficult to intercept, or are users more often ignorant of the many ways other users or providers may eavesdrop on their information? In other words, as technology use increases, does technical literacy also increase, or does overall technical knowledge decrease? For example, a system administrator may not be able to argue that she had a reasonable expectation of privacy when she e-mailed her friend. However, her mother who recently purchased a computer for the first time and has no technical skill may well be able to argue she was entirely unaware of any e-mail security issues. This knowledge may speak directly to the "expectation" element of the Supreme Court's test.[94] However, considering the complex nature of computer systems, there may well be a much stronger presumption that Internet users' unintentional disclosures are indeed protected by this expectation.[95] As the Internet becomes more accessible and easier to use, users require only moderate technical knowledge to participate in the technological revolution. However, the most intriguing – or disturbing – element is that the Supreme Court has yet to find any privacy right for personal information.[96]

B. LEGISLATIVE PROTECTIONS

It is critical to remember that the U.S. Constitution only confers rights regarding governmental intrusions.[97] Private prying is simply

---

Carol M. Bast, *What's Bugging You? Inconsistencies and Irrationalities of the Law of Eavesdropping*, 47 DEPAUL L. REV. 837 (West 1998) (describing how the Communications Assistance for Law Enforcement Act, Pub. L. No. 103- 414, § 202(a)(1), 100 Stat. 4290 finally changed the legal presumption under an earlier act, by specifically protecting the expectation of privacy of cellular and wireless phone users, and noting that traditionally, phone users whose conversations were broadcast over such public airwaves, were expected to have significantly lower privacy expectations than users of land-line phones).

94. *See Hambrick*, 55 F. Supp.2d 504 (1999).

95. *See* Koster, *supra* note 92. *See also* Jonathan R Aspatore & John W. Ellis, IV, *Are You Being Watched? Government and Organizations Voice Concerns over Internet Privacy*, Black Enterprise, Aug. 1999 (West MAGAZINE-C database). The authors of this article describe various ways computers can actively disclose information about the computer's user without that user's knowledge. *Id.* "Cookies," which are small information files that can be automatically saved on the user's machine as they browse the Internet, may track personal information and disseminate it back to the Internet site that originally placed it there. *Id.* It also touches on Intel Corporation's attempt to use the Pentium III chip to automatically collect user information and potentially report it back to the company. *Id.* These automatic data gathering features are generally unknown to the end users and pose a serious privacy threat to people as more and more personal computers are used to store intimately personal information. *Id.*

96. *See* Jonathan P. Cody, *Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation*, 48 CATH. U. L. REV. 1183 at 1193 (Summer 1999).

97. *See* Ballon & Kupferschmid, *supra* note 67, at 144.

not included in the Constitution's or federal acts' privacy protections.[98] However, as people become more sensitive about protecting their personal data,[99] the federal and state governments are drafting stronger protections. California, for example, amended its constitution to include an express right to privacy that protects from both governmental and private intrusions.[100] Indeed, the scope of the amendment is quite broad in that it expressly protects individuals' private data in much the same way the E.U.'s Data Protection Act does.[101]

Federal legislation is likewise broadening its reach to begin expressly providing consumer protections.[102] The Telephone Consumer Protection Act of 1991, for example, allows consumers to opt out of unsolicited marketing calls.[103] However, the Act is only enforceable on a company-by-company basis. To avoid repeated calls, the consumer must specifically request not to be contacted again.[104] In an effort to comprehensively examine consumer privacy issues, the Federal Trade Commission ("FTC") created a congressional report outlining practice guidelines that will likely lead to more cohesive law.[105] Clearly, if additional states move to extend privacy protection in their own constitutions, a person's

98. *See, e.g., id.*, at 143-44; Right to Financial Privacy Act, *infra* note 138 (protecting individuals' financial records from unwarranted government intrusion); *see also* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2711 (protecting individuals' personal data held by internet service providers from unwarranted governmental intrusion).

99. *See, e.g.,* Joel R. Reidenberg, *Symposium: The Legal and Policy Framework for Global Electronic Commerce: A Progress Report*, 14 BERKELEY TECH. L.J. 771, at n. 1 (Spring 1999) (citing surveys that show ". . .82% of those surveyed feel that consumers have lost all control over how companies collect and use their personal information . . . [and] . . . that 78% of those polled found existing statutory protections inadequate to protect privacy.").

100. *See* Ballon & Kupferschmid, *supra* note 67, at 143-44.

101. *See id.* In an action for breach of privacy, the claimant must prove three elements to succeed: the interest breached was legally protected she had a reasonable expectation of privacy under the circumstances, and the offender's act was a serious invasion of privacy. *Id.*

102. *See* Sarbanes, 145 CONG. REC. S554-01, *supra* note 54.

103. *See* Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (West 2000).

104. *See* Stephanie Gallagher, *Telemarketers, Buzz Off! Telephone Consumer Protection Act helps Protect against Telemarketers*, KIPLINGER'S PERS. FIN. MAG., Apr. 1999. The Telephone Consumer Protection Act (TCPA) does have teeth, however. *Id.* It requires that phone solicitors allow people to be put on a do-not-call list, that they not call before or after set times of day, that the caller must provide their name, the company name, address and phone number. *Id.* Each violation of an individual element of the act gives the contacted person the right to sue for up to $500. *Id.* In other words, if a company violates three of the requirements in a single call, the recipient of that call could potentially sue for $1,500. *Id.*

105. *See* Martha K. Landesberg, Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) <http://www.ftc.gov/reports/privacy3/toc.htm>.

fundamental right to protect his or her privacy will become more deeply rooted in our society.

State actions, coupled with the federal government's increasing interest in protecting consumer rights as evidenced by the newer acts and reports, are moving the U.S. slowly towards a more comprehensive notion of the right to privacy and consumer protection. When Senator Sarbanes introduced the Financial Information Privacy Act of 1999, he summarized the problem by contrasting legislation such as the Cable Communications Policy Act with the general state of data protection law in this country, and he noted that while it is now illegal to disclose an individual's cable television selections, companies can freely disclose a person's financial transactions.[106]

C. JUDICIAL PROTECTIONS

While the notion of a right to privacy is flourishing,[107] Constitutional protections are limited[108] and federal legislation is piecemeal.[109]

---

106. *See* Sarbanes, 145 CONG. REC. S554-01, *supra* note 54, at S614.

> Concern over the privacy of personal data is sharpening as the problem appears in more and sometimes unexpected contexts-everything from employer testing of people's genetic predisposition to resale of their online reading habits or their bank records. When the data are medical or financial, everyone but the sellers and resellers seems ready to agree that people should have some measure of control over how and by whom their data will be used.
>
> Congress has protected citizens' privacy on prior occasions. In response to public concerns, Congress passed privacy laws restricting private companies' disclosure of customer information without customer consent, such as in the Cable Communications Policy Act and the Video Privacy Protection Act. Yet while video rentals and cable television selections are prohibited by law from being disclosed, millions of Americans' financial transactions each day have no Federal privacy protection.

Id.

107. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1976).

> In 1890 a noted article, by Warren and Brandeis, The Right to Privacy, in 4 Harv.L.Rev. 193, reviewed these cases, and concluded that they were in reality based upon a broader principle that was entitled to separate recognition. Although this conclusion was first rejected in Michigan and New York, it was accepted by the Georgia court in Pavesich v. New England Life Insurance Co. (1905) 122 Ga. 190, 50 S.E. 68. Following that decision, the existence of a right of privacy is now recognized in the great majority of the American jurisdictions that have considered the question.

Id.

108. *See* Kirchner, *supra* note 62.

109. *See* Ballon & Kupferschmid, *supra* note 67, at 140.

> U.S. Data privacy law is comprised of a patch-work of constitutional, statutory and common law privacy rights that afford substantial protection in very narrow areas. Privacy rights are recognized under U.S. law in specific circumstances (such as in the context of criminal investigations or in response to intrusive snooping by strangers), for particular categories of information (such as tax returns, personal financial data or medical records) or for specific classes of people (such as children). By comparison, the protections afforded by U.S. privacy laws are less comprehensive than those mandated by the European Union's Privacy Directive.

Since these areas of the law provide only small pockets of protection, the state of case law on such matters becomes more important. The Restatement (Second) of Torts acknowledges the invasion of privacy as a tortious offense, whether the intrusion is a physical invasion, or a virtual one.[110] Generally, the four causes of action for invasion of privacy – unreasonable intrusion or interference with solitude, public disclosure of private facts, the appropriation of a name or likeness, and false light publicity – may all be implicated in data protection cases.[111] For example, using a web site to publish private information about another person for the sole purpose of discrediting or embarrassing him would clearly be a tortious invasion of privacy. The case law, however, illustrates that depending on the circumstances, an actionable invasion of privacy regarding personal data is often hard to prove.[112] It appears that civil judges, as did the Supreme Court justices, struggle to identify the particular rule of law that should apply in general privacy issues when a wrong is recognizable, but the rule that makes it wrong is not easily identifiable.[113]

Id.

110. *See* RESTATEMENT (SECOND) OF TORTS, *supra* note 107, at §652B. The Restatement defines the offense of intrusion upon seclusion as "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Id.* The comments make it clear that this includes a physical invasion, such as entering a person's home, an invasion accomplished through the offender's senses, such as eavesdropping, wiretapping, or peering in someone's windows, or by some investigation or examination of a person's private affairs, such as reading someone's mail or accessing their bank account information. *Id.*

111. *See id.*

112. *See, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351 (1995) (holding that it was not a tortious appropriation of personal information to include credit card holder's names in categorized marketing mailing lists); *see also* Biddle v. Warren General Hosp., 86 Ohio St. 3d 395 (1999) (holding that it is a breach of patient confidentiality rather than an invasion of privacy when a doctor tortiously provides nonpublic information to a third party who does not have the privilege to receive such information). *But see Dwyer*, 652 N.E.2d 1351 (citing Douglass v. Hustler Magazine, 769 F.2d 1128 (7th Cir. 1985)) (holding that the commercial nonadvertising use of a person's photograph is a valid appropriation claim in Illinois).

113. *See, e.g, Biddle*, 86 Ohio St. 3d at 400, where the court, which was dealing specifically with a doctor's breach of patient confidence, wrote a rather remarkable passage reflecting on such judicial struggles:

> In much the same way as trying to fit a round peg into a square hole, courts have utilized theories of invasion of privacy, defamation, implied breach of contract, intentional and negligent infliction of emotional distress, implied private statutory cause of action, breach of trust, detrimental reliance, negligence, and medical malpractice. Invariably, these theories prove ill-suited for the purpose, and their application contrived, as they are designed to protect diverse interests that only coincidentally overlap that of preserving patient confidentiality. These courts, therefore, often find themselves forced to stretch the traditional theories beyond their reasonable bounds, or ignore or circumvent otherwise sound doctrinal limitations, in order to achieve justice within the parameters they have set for them-

The catch point for many cases involving data privacy is not in having to meet the standard that the unreasonable intrusion must be an intentional intrusion that is "highly offensive to a reasonable person."[114] Instead, one of the most significant problems is defining whether any of the data was voluntarily disclosed.[115] If the aggrieved party in any way "voluntarily" released that information, the offender's liability might be relieved, which is a surprisingly broad point of law.[116] Consumers releasing data for a specific purpose, such as using a credit card to make a purchase or giving personal information to open an ISP account, may be surprised that their acts are interpreted as having "volunteered" their information to the open market. This purpose-specific released data is a free license to any entity that wants to use the individual's data for virtually any purpose,[117] because it has become public information.[118] Where privacy is concerned, it appears that possession is indeed nine-tenths of the law.[119] A tortious invasion is much harder to define under these circumstances. For example, if a person discloses his sexual orientation to

---

selves. In so doing, they rely on various sources of public policy favoring the confidentiality of communications between a physician and a patient, including state licensing or testimonial privilege statutes, or the Principles of Medical Ethics of the American Medical Association (1957), Section 9, or the Oath of Hippocrates. Some note that while public policy considerations are a sound enough basis to support liability, a more appropriate basis can be found in the nature of the physician-patient relationship itself, either because of its fiduciary character or because it is customarily understood to carry an obligation of secrecy and confidence. Slowly and unevenly, through various gradations of evolution, courts have moved toward the inevitable realization that an action for breach of confidence should stand in its own right, and increasingly courts have begun to adopt it as an independent tort in their respective jurisdictions. (Citing a vast array of decisions illustrating these judicial struggles.)

Id.

114. *See* RESTATEMENT (SECOND) OF TORTS, *supra* note 107, at §652B.

115. *See, e.g., Dwyer*, 652 N.E.2d 1351.

116. *See id.*

117. *See id.*

118. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (discussing privacy protections, the court stated "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection"). Even though the focus here has been on individual data privacy rights, companies, and their secrets, are also vulnerable. *Id. See, e.g.,* Ballon & Kupferschmid, *supra* note 67, at 99. "Disclosure destroys the secret. The U.S. Supreme Court held that, 'upon disclosure, even if inadvertent or accidental, the information ceases to be a trade secret and will no longer be protected.' Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475-76 (1974)." *Id.*

119. *See, e.g.,* Couch v. United States, 409 U.S. 322 (1973) (finding that ownership and possession of information are extremely important distinctions). Where a person voluntarily turns over possession of records, his or her privacy interest in that information dissolves. *Id.* Here, the defendant was barred from claiming Fifth Amendment protection in regards to tax records turned over to the defendant's personal accountant. *Id.* Once the data was out of the defendant's possession, she no longer possessed it and lost her privacy interest to the degree that she could no longer claim the protective right). *Id.*

a small group of people in private gay-rights-oriented e-mails, and subsequently discovers that a hate group has published his name and is disseminating it throughout the community, has his right to privacy completely dissolved because of the earlier e-mail discussions? Would it be dissolved if he only disclosed his orientation to a small group of people at the office? The problem is that the scope of disclosure is not well defined. The courts or legislature must come to some agreement as to what exactly constitutes disclosure. Disclosure must then be defined so that the boundaries are clear for individuals, consumers, and companies.

There are a number of cases that illustrate the difficulties of data protection law in this country. In a relatively early Supreme Court case, *Whalen v. Roe*, at issue was a statute requiring prescription information on abused drugs to be logged in a state database.[120] The Court upheld the statute, but acknowledged a privacy interest in the data as well as an inherent threat to privacy posed by this type of massive database containing personal information.[121] The court in *Dwyer v. American Express Co.* did not extend the idea expressed in *Whalen's* dicta and instead held that voluntary use of a credit card is a voluntary disclosure sufficient to allow credit card companies to freely disseminate data about their clients.[122] The idea expressed in *Whalen*, that databases were inherently prone to threatening privacy, was not sufficiently persuasive to protect the commercial credit card user. In fact, an earlier holding, in *Shibley v. Time, Inc.*, the Ohio Court of Appeals held that commercial data collections such as marketing lists are only valuable when they contain the data on many people, and therefore an individual's data by itself has no commercial value.[123] This being the case, an individual cannot successfully prevent his personal data from being disseminated by arguing a taking has occurred or that he is permanently deprived of the commercial value of that data.[124] This holding makes a misappropriation challenge virtually impossible.[125] It used to be the case that marketing

120. *See* Whalen v. Roe, 429 U.S. 589 (1977).

121. *See id.* It is notable that, while the Court's opinion regarding data privacy was a positive step, it somewhat diminished the impact of the idea by further stating that a right to collect such information is usually accompanied by a "duty to avoid unwarranted disclosures." *Id.* at 605. The implication appears to be that the threat to privacy posed by databases is minimized where the collector has a protective duty. *Id.* While they were correct in the context of medical information, financial and other personal data appears to be much more vulnerable. *Id. See generally* Sarbanes, 145 CONG. REC. S554-01, *supra* note 54.

122. *See* Dwyer v. American Express Co., 652 N.E.2d 1351 (1995).

123. *See* Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975).

124. *See id.*

125. *See* Koster, *supra* note 92, at 10. The article holds some hope, however, that as technology improves our ability to gather and link vast amounts of data, the courts will begin assigning more actual worth to an individual's personal information. *Id.* It seems

companies only saw the aggregate numbers and base generalizations regarding buying habits. Before computers, it would have been very difficult to decompose the data and access a single person's statistics. With the advent of powerful search software and data-mining systems, these massive marketing databases can be made as homogeneous or granular as the operator wants. Magazine publishers, for example, can now customize a magazine's ads for specific subscribers.[126] One person might see a perfume ad on page 27, while her neighbor has a men's clothing ad on the same page.[127] Indeed, both can easily be customized to include the subscriber's name as part of the ad's text.[128] Given the extreme detail that can be gathered about an individual, and given that the new breed of marketers feels personalized marketing is worth the expense, the U.S. Supreme Court will be forced to reexamine the holding that individual data is worthless while only aggregate data is valuable.

As for whether or not statutory protections regarding privacy will be upheld in the courts, particularly privacy against governmental intrusion, legislation leaves many holes.[129] The Electronic Communications Privacy Act ("ECPA") requires that a government organization must have a warrant, court order, or the like, before getting access to an individual's personal information from an electronic communications or service provider, such as the phone company or an ISP.[130] In the event that the government improperly requests or the company improperly discloses the data, the individual has a civil cause of action against the violator.[131]

---

unlikely that, given how hard some commercial entities are fighting for unfettered access to individuals' personal information, the courts can persist forever in holding that one person's data is worthless in and of itself. *Id.*

126. *See* Interim Technology, Systems Engineering Division, Dec., 1998. (Proposal and systems documentation on file with the author). This company has designed and installed just such a customizing system in a number of magazine and newspaper printing plants, such as R.R. Donnelly. *Id.*

127. *See id.*

128. *See id.*

129. *See, e.g.*, United States v. Hambrick, 55 F. Supp.2d 504 (1999) (holding that the data gathered by law enforcement officials on what turned out to be an invalid warrant, was nonetheless admissible at trial); *see also* Tucker v. Waddell, 83 F.3d 688 (1996) (holding that the plaintiff could not sue the city under the Electronic Communications Privacy Act, even though the subpoena was not valid, because the data was technically publicly available anyway).

130. *See* The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2711 (1988). The Act requires a governmental entity to have a valid subpoena, warrant, court order, or an individual's permission before the communications service provider may disclose the individual subscriber's information. *Id.* at § 2703(c)(1)(B). A violation of the act expressly allows a private cause of action against the party that "engaged in" the violation. *Id.*

131. *See Tucker*, 83 F.3d at 690. In this case, the plaintiff brought suit against officers for improperly acquiring her personal subscriber information from the phone company. *Id.*

A recent case, *United States v. Hambrick*, however, illustrated that these express provisions of the ECPA may be frustrated by court holdings.[132] Officials served warrants on an ISP in order to gather personal information on Hambrick – warrants that were later deemed improper.[133] Hambrick sought to suppress the information because it violated his Fourth Amendment rights alleging, amongst other things, that the government's breach of the ECPA rules indicated he had a privacy expectation regarding the data.[134] The court held, however, that the ECPA did not create an expectation of privacy sufficient to sustain the Fourth Amendment protection.[135] The court held that the ISP was allowed to freely disseminate the data in question to any entity *other* than the government.[136] Therefore, the data was in the public domain and the ECPA was not violated.[137] This reasoning appears to be directly contradictory to the intent of the ECPA, which is to prevent governmental intrusion into personal records held by electronic service and communications providers – providers like ISPs. It means that government officials can subvert the reach of the ECPA by simply providing the company with documentation that is alleged to be a valid warrant. If an invalid warrant works as well as a valid one to gather the data, as was

---

However, instead of making her claim under the sub-section that controls the government's actions, the plaintiff incorrectly based her argument on the provision governing the company's actions. *Id.* Therefore, the court found against the plaintiff for failure to state a claim. *Id.* Given this holding, the reviewing court never had to address issues such as whether or not it was possible for the plaintiff to sustain a claim (had she, in fact, filed under the proper sub-section), given that the data acquired by the authorities was technically in the public domain. *Id.* The lower court found that because the company was expressly allowed to disseminate the data to any non-governmental entity, the information was publicly available, and therefore the Act was not violated. *Id.* Since the Act expressly forbids governmental interests access to data without the proper legal authority while it simultaneously allows the companies in question to freely disseminate the same data to any non-governmental entity, this reasoning would seem to entirely invalidate the purpose of the Act.

132. 55 F. Supp.2d 504.

133. *See id.*

134. *See id.*

135. *See id.*

136. *See id.* The exact language of the Act is that "a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity." 18 U.S.C. § 2703(c)(1)(A) (West 1999). The *Hambrick* Court stated that "[t]he fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information." *Id.* The Act attempted to protect from government intrusion without otherwise limiting the freedom of the companies to do what they like with people's personal data, and the court appears to expressly take advantage of that contradiction of purpose. *Id.*

137. *See Hambrick*, 55 F. Supp.2d 504.

the case in *Hambrick*, there would seem to be a serious flaw in the Act.[138] As a short term solution, Congress can amend the ECPA to address the issue of invalid warrants and define the implications. This would avoid the circular logic that found a way to use data privacy legislation as a shield protecting bad warrants. The long term solution, however, will have to be one that weaves the various U.S. data privacy protections into a single cohesive legal rule.

The fact that the ECPA does not protect individuals' privacy from anyone besides the government may prove to be a fatal flaw. More disturbing, the ECPA models closely after the Right to Financial Privacy Act ("RFPA").[139] There may be the same vulnerability in that Act as well, and any others that bar governmental intrusion while allowing unfettered non-governmental distribution of the data. Fortunately, Congress appears increasingly conscientious about the privacy concerns of its constituents, at least where specific types of information, such as financial and medical records, are concerned.[140] However, the problem of multiplying a flaw by modeling one rule on another instead of on consistent legal theory or policy, can only be mended by the long-term solution of developing consistent legal thinking on data privacy.

There also appears to be an unexpected flip-side to this issue. In one case, a governmental organization attempted to hide behind privacy legislation, the Privacy Act of 1974,[141] to *avoid* providing individual data for necessary and constructive purposes.[142] The U.S. Navy did not want

---

138. *See id.*

139. Tucker v. Waddell, 83 F.3d 688 (1996), which discussed the close relationship of the two Acts at length. *See also* Right to Financial Privacy Act, 12 U.S.C. 3401 (West 2000).

140. *See* Sarbanes, 145 CONG. REC. S554-01, *supra* note 54, at S615. Mr. Sarbanes specifically stated that Americans should have the right to know their personal financial data is kept private, and expressed protective concepts that strongly parallel those embodied in European law:

> Every American should know whether the financial institution with which he or she does business undertakes to sell or share that personal sensitive information with anyone else. Every American should know who would be obtaining that information, and why. Every American should have the opportunity to say "no" if he or she does not want that confidential information disclosed. Every American should be allowed to make certain that the information is correct. And these rights should be enforceable.

Id.

141. Privacy Act of 1974, 5 U.S.C. § 552a (West 2000) (requiring federal agencies to limit the collection of personal information, to maintain the accuracy of that information, and to ensure its security).

142. *See* Federal Labor Relations Authority v. U.S. Navy, 966 F.2d 747 (1992). At issue was the Navy's attempted invocation of the Privacy Act in order to withhold the names and addresses of employees regarding the collective bargaining unit of the Federal Labor Relations Authority.

to turn over names to a collective bargaining group.[143] The claimants who needed the data argued, however, that two exceptions within the Act allowed the distribution: the Freedom of Information Act exemption[144] and the "routine use" exception.[145] The court held that the Freedom of Information Act in and of itself allowed the disclosure of the necessary names and addresses.[146]

Clearly, in regards to personal data, notions of Constitutional privacy protections are vague[147] and lack concise Constitutional interpretations.[148] Further, statutory protections are overly narrow[149] and potentially self-contradictory in their legal interpretation,[150] and tort protections are uneven at best.[151] The legal approach to protecting data

---

143. *See id.*

144. 5 U.S.C. § 552(b)(6).

145. 5 U.S.C. § 552a(b)(2) and (3).

146. *See Federal Labor Relations Authority,* 966 F.2d at 754. The court stated that "the privacy interest of government employees in their home addresses did not outweigh the strong public interest in collective bargaining mandated by the Labor Statute and the FOIA's policy in favor of disclosure." *Id.*

147. *See* Griswold v. Connecticut, 381 U.S. 479 (1965). The Supreme Court's attempt to define the Constitutional source for privacy protection in the *Griswold* case wanders through myriad Amendments, ultimately basing the implied right to privacy on other implied Constitutional rights. *Id.*

148. *See, e.g.,* Cody, *supra* note 96. The article notes that the Supreme Court has "yet to hold that protection exists for an individual's right to privacy of personal information. . ." *Id.* at 1193. The article relies on Fred H. Cate, *Privacy and Telecommunications,* 33 WAKE FOREST L. REV. 1, 18 (1998) for support in "arguing that the Supreme Court's interpretation of individual privacy protection is confused and limited when compared to explicit constitutional rights." *Id.* at n. 38.

149. *See, e.g.,* Cody, *supra* note 96 at n. 69.

> See infra Parts I.C.1-2 and accompanying notes (discussing United States laws governing the collection, use, and disclosure of personal identifiable information and the industry to which they apply); see also Cate, Privacy, supra note 42, at 99 (stating that United States informational privacy laws apply only to specific categories of information users); Gindin, [Susan E. Gindin, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 San Diego L. Rev. 1153, 1170 (1997)] supra note 12, at 1196 (explaining that Congress' approach to protection of personal identifiable information has resulted in "piecemeal" legislation that addresses only specific privacy needs).

Id.

150. *See* National Information Infrastructure Task Force, Options for Promoting Privacy on the National Information Infrastructure, Draft for Public Comment, Apr. 1997, (visited Oct. 12, 1999) <http://www.iitf.nist.gov/ipc/privacy.htm>. "The federal system of data protection, though comprehensive, is criticized, however, as a 'paper tiger' with significant enforcement and remedial deficiencies." *Id.*

151. *See, e.g.,* Koster, *supra* note 92, at 10. In attempting to quantify tort protections for data privacy, the author reviews the various invasion of privacy causes of action that may or may not stand to protect data, discussed decisional contradictions, and speculated on additional causes of action that may be called upon to protect an individual's control over the collection and use of his or her own data. *Id.* "Other doctrines, such as fraud, negligence, breach of confidentiality, breach of contract, unjust enrichment, infliction of emo-

privacy in the U.S. is a nearly random collection of overly-broad or narrow rules that ultimately protect only very specific data privacy rights.[152] Collectively mending all of these inconsistencies may require extensive time, and legislative stop-gaps will certainly have to be developed to shore up the leaky legal umbrella. However, the U.S. must recognize the need for a single solution or risk losing international trade while feeding internal alienation.

D. Commercial Self-Policing Protections

Because the legal basis for data protection in the U.S. is uneven at best, the official stated policy of the U.S. government strongly encourages companies to self-regulate and attempt to satisfy the Directive requirements that way.[153] The strategy appears to be aimed at avoiding chilling the U.S. economy and instead relying on the free market to encourage businesses to respect consumers' privacy rights.[154] It is a familiar U.S. economic theory of evolution. If consumers care about privacy, they will patronize companies that care about privacy.[155] If companies do not evolve to accommodate those customers, the companies will become extinct.[156] The proposal was to create a standard of conduct that companies voluntarily comply with in order to become considered a "safe harbor."[157] However, despite the continual efforts of the U.S. govern-

---

tional distress, and trespass, could also come into play depending on the relationship between the individual and the invader and the particular facts of the case." *Id.*

152. *See* Cody, *supra* note 96, at n. 192, likening the U.S. legal position on data privacy to a patch-work quilt.

153. *See* Joel Brinkley, *Gore Outlines Privacy Measures, but Their Impact Is Small*, N. Y. Times, Aug. 1, 1998 < http://www.nytimes.com> (resulting from search for gore and "medical records" and privacy). "But the Administration chose not to offer broad new ideas for protecting the privacy of adults on line, an issue important to many in Congress and to public-interest groups. Gore announced instead that, for now, the Administration would leave industry to regulate itself." *Id.*

154. *See* Reidenberg, *supra* note 99, at 775. "The theory holds that the marketplace will protect privacy because the fair treatment of personal information is valuable to consumers; in other words, industry will seek to protect personal information in order to gain consumer confidence and maximize profits." *Id.*

155. *See id.*

156. *See id.*

157. The United States Mission to the European Union, *Thompson: The EU Committee of AMCHAM*, (Dec. 3, 1998) <http://www.useu.be/ISSUES/mozelle123.html> [hereinafter *Thompson: The EU Committee of AMCHAM*].

> It is presently envisioned that organizations qualifying for the safe harbor would have a presumption of adequacy and data transfers from the EU countries to them would continue. Organizations could come within the safe harbor by self-certifying that they adhere to these privacy principles. While the specific terms of the safe harbor arrangement are still under discussion with the European Community, the U.S. believes that it provides a framework for compromise because it would be deemed acceptable by all member States and would provide for streamlined and expedited transfer approvals and dispute resolution.

ment to encourage private commercial reforms, little concrete progress was made until recently, the E.U. continues to withhold its approval, and major U.S. and European consumer groups reject the safe harbor proposal.[158] Quite simply, earlier proposals lacked teeth. Not only did it lack any mention of an enforcing body, the proposal did not carry any repercussions for violators. Considering that consumers are generally more interested in being protected against the less ethical companies, the first "safe harbor" proposals fell far short of providing protection. It was little more than a suggestion to companies that they be conscientious of private data. Indeed, this was the sort of proposal that should have been put forth by trade organizations and business lobbyists, not by the federal government as a solution to an increasingly critical legal problem. The more recent draft of the safe harbor proposal seems to be making some headway.[159] This latest proposal includes enforcement options. While the first round of protection is still voluntary – companies simply agree to abide by the E.U.'s privacy principles – the new proposal adds the threat of prosecution for any U.S. company that agrees and then violates their agreement.[160] However, considering that the injured party is necessarily an ocean away, the effectiveness of the proposal's "teeth" remains to be seen.

In 1987, President William Clinton strongly promoted an administrative preference for this style of private management to combat serious

---

Id.

See also International Trade Administration, *International Safe Harbor Privacy Principles, Draft*, Apr. 19, 1999. <http://www.ita.doc.gov/ecom/shprin.html> (updating the Nov. 1998, Safe Harbor proposal and outlining in detail the privacy principles proposed by the U.S.); *see also Aaron: French and American Business Community, supra* note 51 (commenting that the proposed safe harbor principles offer a mutually acceptable means of ensuring adequate privacy protection for E.U. data, although the E.U. itself has not yet agreed).

158. *See Oversight Hearing on Electronic Communications Privacy Policy Disclosures Before the Subcomm. on Courts and Intellectual Property Comm. on the Judiciary* (1999) [hereinafter *Oversight Hearing on Electronic Communications*] (paraphrasing the statement of Marc Rotenberg, Director, Electronic Privacy Information Center) <http://www.epic.org/privacy/internet/Epic_testimony_ 599.html> (describing U.S. efforts to promote self-regulation, E.U.'s negative reactions, and detailing international consumer protection group objections to private industry policies, which are ". . .typically incomplete, incoherent, and unenforceable"). *See also Thompson: The EU Committee of AMCHAM, supra* note 156 (stating, "[i]n June of this year [1999], the FTC issued a report on Internet privacy which showed that industry's progress toward self-regulation was practically nonexistent").

159. *See* European Union, *Data Protection: European Commission Endorses "Safe Harbor" Arrangement with United States* (visited May 13, 2000) <http://www.eurunion.org/news/ press/2000/2000014.htm> [hereinafter *Data Protection*].

160. *See id.* The misrepresentation and deceptive trade practice clause, §5 of the U.S. F.T.C. Act, is primarily implicated in this prosecutorial threat. *Id.*

consumer data protection issues.[161] However, as it became painfully clear that leaving privacy protection in the hands of the data collectors is not meeting expectations, the Clinton administration backed away somewhat from the strictly *laissez-faire* policy it has expressed since the late 1980's.[162] In a recent speech, President Clinton discussed the Financial Privacy and Consumer Protection Initiative, which is founded on several principles, including strengthening privacy protections for financial and medical records, and to requiring heightened public disclosure standards for companies.[163] Nevertheless, there was still a fairly strong emphasis on the administration "partnering" with business.[164] There was little information about the actual power of the initiative and none about its implementation and enforcement.[165] Another sign that the official policy was moving towards a more serious approach to protecting personal information, President Clinton appointed a Chief Counselor for Privacy, Peter Swire, an Ohio State University law professor.[166] However, given the enormous scope of the work facing this new appointee, the initiative is not nearly staffed to the levels the E.U. has devoted to the role.[167] President Clinton is in a unique position to state a unified policy towards data protection, and he has the opportunity to create the beginnings of an infrastructure that will support and protect Internet trade and privacy. However, this unbalanced policy of promoting commercial self-regulation, while at the same time taking feeble steps towards governmental oversight, does nothing to foster international confidence in U.S. data protection. The E.U. appears ready to attempt to get Mem-

161. *See* Reidenberg, *supra* note 99, at 775. "The [Clinton] Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy." *Id.* [Citing] William J. Clinton & Albert Gore, Jr., A Framework for Global Electronic Commerce (July 1, 1997), (visited Sept. 19, 1998) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> § at 14 (Issue 5). *Id.* at n. 15.

162. *See Thompson: The EU Committee of AMCHAM, supra* note 156. "The following month [July 1999], the entire [Federal Trade] Commission testified before the U.S. House of Representatives and indicated that, if substantial progress were not made soon, additional governmental authority through legislation would be appropriate and necessary."

163. *See* President William Clinton, The United States Mission to the European Union, *Remarks by the President on Financial Privacy and Consumer Protection* (May 4, 1999) <http://www.useu.be/ISSUES/clinton0521.html>.

164. *See id.*

165. *See id.*

166. *See* Koster, *supra* note 92, at 11.

167. *See id.* "Swire is to coordinate administration initiatives, work with states, and serve as an international contact for privacy matters . . . . However, Swire will have only two dedicated staff members and will not directly handle consumer redress . . . . Contrast this arrangement with that of the Netherlands and United Kingdom, both of whom have independent privacy agencies of 50- and 100- plus employees, respectively, to take complaints and initiate legal action against privacy violators . . . ."

ber State approval for the safe harbor proposal,[168] but even if the policy is accepted and European consumers are truly protected, it speaks poorly for U.S. protection of U.S. consumer data. What will become of the safe harbor policy if it serves to protect European citizens at a level only hoped for by U.S. citizens? The administration's policy confuses the internal legal struggle to develop a comprehensive policy. While the steps toward establishing a Privacy Counselor are positive, they are simply another facet cut on the face of an unnecessarily complicated and nearly schizophrenic U.S. public policy.

Still, it is technically possible to let each U.S. company develop its own solution.[169] In fact, there are a number of ways, apart from the formal safe harbor proposal, that companies can comply with the Act in the absence of the E.U. declaring U.S. compliance.[170] For example, any U.S. company with European ties can include a clause in its contract

---

168. *See Data Protection*, *supra* note 158.

169. *See, e.g., City & Commercial: Bridging the transatlantic data divide.* THE LAW., June 7, 1999, *available at* 1999 WL 9132459.

170. *See* Data Protection Directive, *supra* note 19. On matters regarding derogations, the Directive provides as follows:

> 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
> (a) the data subject has given his consent unambiguously to the proposed transfer; or
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
> (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
> 2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
> 3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
> If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the

stating it will wholly comply with the Directive, or it can contact its European customers directly and expressly get permission to use their data.[171] However, if all of the U.S. businesses with foreign customers are required to take these measures – individual one-to-one contract negotiation or express customer contact – they may as well support outright U.S. adoption of the Directive. They will bind themselves to the terms and burdens of the Directive, with none of the U.S. legal consistency to help mediate disputes, and no central U.S. authority to enforce compliance.[172] Every dispute could ultimately end up in federal court, with all of the jurisdictional and international comity problems that suggests.[173]

E. E.U. DATA DIRECTIVE PROTECTIONS

In contrast, whatever might be said about the E.U.'s Data Privacy Directive being commercially restrictive,[174] the uniform protections of-

---

Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

Id.

171. *See, e.g., City & Commercial: Bridging the Transatlantic Data Divide*, *supra* note 168.

172. *See* Filetech v. France Telecom, 157 F.3d 922 (1998). In this unusual case, the U.S. subsidiary of a French marketing list company had taken advantage of a France Telecom listing service to download France Telecom's phone directory for free. *Id.* However, Filetech could not use the data without first purging the list of the people who denied permission to use their data for marketing purposes. *Id.* Filetech sued France Telecom in U.S. federal court in an attempt to force them to produce the list of those subscribers who disallowed marketing uses. *Id.* Ironically, France Telecom offered the full marketing list for a fee, but Filetech was apparently not interested in compiling the data that way. *Id.* A lower court denied France Telecoms attempt to dismiss for lack of subject matter jurisdiction, but did dismiss based on the fact that, if they forced France Telecom to produce the list of non-marketing subscribers, they would be forcing France Telecom to break French law, including data privacy law. *Id.* The higher court, however, remanded the case to determine whether or not the federal court did have subject matter jurisdiction, and whether or not there was truly a conflict between U.S. and French law. *Id.* The case illustrates the enormous difficulty that will likely be encountered in adjudicating international data protection disputes where there are inconsistencies between U.S. and European law.

173. *See id.*

174. *See* Lillington, *supra* note 15.

So far, seven EU states have implemented the directive, which, for the past year, has been the subject of a major row between the US and the EU because of its data-handling restrictions. Under the terms of the directive, non-EU countries would have to handle data from EU citizens under the same terms that apply in the EU.

fered by that Directive appear much easier to interpret and apply, and result in more consistent holdings[175] than do the U.S. rules on data protection.[176] Coupled with other E.U. acts, the European data protection laws offer comprehensive privacy protection regarding both data access and use from commercial, governmental, and fundamental human-rights perspectives.[177]

The heart of the Directive lies in its broad scope of definitions[178] and straightforward list of what is and is not allowed regarding processing personal data.[179] Interestingly, many of the protections enumerated by the Directive are also present in U.S. data protection legislation, such as the Children's Online Privacy Protection Act ("COPPA").[180] The E.U.'s

---

> In particular, the US has resisted giving European consumers access to data records held on them by US companies. Access to all data records is a primary provision of the 1988 and 1998 Data Protection Acts.

Id. at 1.

175. *See, e.g.,* R. v. Department of Health Ex. p. Source Informatics Ltd., Lloyd's Rep. Med. 264, 1999, *available in* 1999 WL 394604 (Q.B., May 28, 1999) (holding that it is illegal to release drug prescription or dispensing information to a third-party for commercial purposes without the consent of the individual patients, even where patients are anonymous, since it is vital that people be able to seek medical help ". . .without fear that information concerning their consultation would be released without their permission."); British Gas Trading Ltd. v. Data Protection Registrar, Info T.L.R. 393, 1998, *available in* 1999 WL 276828 (Data Protection Trib., Mar. 24, 1998) (holding that it was not sufficient for the gas company to simply mail leaflets inviting customers to opt out of having their personal data used for purposes other than those relating to their gas service, but would have been sufficient had the leaflets described the type of marketing proposed and then given customers the opportunity to either object or consent).

176. *See* Reidenberg, *supra* note 99, at 782. The European Union approached the legal issue of data privacy by adopting comprehensive rules based on a rights-based model of privacy, as opposed to the U.S. market-based model. *Id.* This comprehensive framework provides a uniform legal standard for all of the Member States. *Id.*

177. *See, e.g.,* European Convention on Human Rights 1950, art. 8, which protects an individual's right to respect for family and private life and is raised in respect to issues such as medical record disclosures. *Id. See also* Z v. Finland, 25 E.H.R.R. 371, 1998, *available in* 1997 WL 1018421 (CLC) (Eur. Ct. H.R., Feb. 25, 1997); DPP v Bignell, 1 Cr. App. R. 1, 1998, *available in* 1997 WL 1016155 (CLC) (Q.B.D., May 16, 1997) (holding that the Data Protection Act 1984 only prohibits unauthorized *use* of personal data, while unauthorized *access* is prohibited by the Computer Misuse Act 1990).

178. *See* Data Protection Directive, *supra* note 19, at ch. 1, art. 2(a). Personal data, for example, is defined as "any information relating to an identified or identifiable natural person." *Id.* An identifiable person is one who can be identified, directly or indirectly from the data. *Id.* at 2(b). The definitions, and there are only eight of them, are very broad and simple at the same time. *Id.*

179. *See* Data Protection Directive, *supra* note 19.

180. Children's Online Privacy Protection Act, 15 U.S.C.A. § 6501 (West 1999) (prohibiting the collection or processing of personal data – data that can identify the child – from a child under the age of thirteen unless the collector has verifiable parental consent); *See also15* U.S.C.A. § 6502 (West 2000) (prohibiting Web or online operators from directing queries towards children to gather personal data; requiring the site to affirmatively disclose what information is being gathered; requiring that the operator provide, at a parent's

Directive and U.S.'s COPPA are perhaps the most similar of the E.U. and U.S. privacy protection acts, except that the COPPA only covers children under the age of thirteen.[181] For example, COPPA requires data collectors to get express parental permission in order to gather personal data on a child, to give parents access to their children's personal data, and to allow parents the right to refuse to let the data collector continue using a child's data.[182] Strikingly, a number of these elements of COPPA are nearly identical to the elements of the Data Protection Directive that U.S. companies are most adamantly against.[183] For example, U.S. companies object to universal express consent for use or dissemination, free access to the actual data, and compliance dictated by legislation instead of self-regulation.[184] Elements of some of the other U.S. acts likewise parallel these similarities between the two laws, but their scope is generally very narrow[185] – far too narrow to appease the E.U. negotiators[186] who continue working with U.S. officials to strike a uniform agreement regarding the breadth of protection required which "ensures an adequate level of protection."[187] Without forcing a more conservative shift in U.S. commercial use of personal data, there is little or no incentive for companies to abandon the huge monitory incentives offered by data mining. Despite U.S. commercial objections, the government or courts must compel them to begin complying.

Data protection laws in Europe have worked successfully for nearly two decades in allowing its citizens to protect and control their personal information, while acknowledging that the rules should not put excessive

---

request, a description of the specific data gathered, an opportunity for the parent to refuse access to or continued use of the child's information; requiring the operator to allow a parent to obtain the child's personal information; prohibiting the operator from enticing a child to provide unnecessary information in order to participate in a game or other online activity; and requiring the operator to develop and maintain procedures to ensure the privacy of data that is in his or her possession).

181. 15 U.S.C.A. § 6501.

182. *See id.*

183. *See* The United States Mission to the European Union, *Remarks of David L. Aaron Under Secretary of Commerce for International Trade, Netherlands* (June 11, 1999) <http://www.useu.be/ISSUES/aaron0618.html> [hereinafter *Aaron: Netherlands*].

184. *See id.*

185. *See, e.g.*, Koster, *supra* note 92, at 10.

> The Fair Credit Reporting Act of 1970 (FCRA) governs consumer credit reporting agencies. [FN36] Courts have thwarted the FTC's attempts to use the FCRA to prevent credit bureaus from selling information to marketers. The U.S. Court of Appeals for the D.C. Circuit held that only information collected "to serve as a factor in determining credit eligibility" falls under the prohibitions of the Act.

Id.

186. *See Aaron: USIA Foreign Press Center Briefing*, *supra* note 29.

187. Data Protection Directive, *supra* note 19, at ch. 4, art. 25, S. 1.

burdens on business or law enforcement.[188] Germany, for example, had data privacy legislation in place since at least the early 1980's, and the application of the German Data Privacy Act acknowledges "reasonableness" as an important element in a company's compliance.[189] For example, like the newer Data Protection Directive, the older German Act required a company to provide a listing of the third-parties that receive a given individual's personal data.[190] However, the Act's application was held in check in a number of ways, including limiting the disclosure to third-parties that "regularly" receive the data (as opposed to every entity that received the data), and noting that prohibitively costly disclosures are likewise not required.[191] Application of the laws also appear to balance governmental needs with personal privacy concerns. Data that is legitimately needed by a governmental body or social agency, such as information required for a court case or an insurance claim, can be disclosed, but in the interest of the individual's privacy, the information is subject to strict rules regarding its security.[192] There are even restrictions on governmental officials regarding what data can be gathered and on what constitutes impermissible access to data that has otherwise been legitimately gathered.[193] European court holdings, which cross na-

188. *See* Re Personal Data Communication (Case III ZR 187/82 Bundesgerichtshof (German Federal Supreme Court) [1985] ECC 403 15 DEC. 1983 (reiterating that a person has the right to know what persons or entities regularly receive the individual's personal data from the given data collector).

189. *Id.*

190. *See id.*

191. *See id.*

192. *See, e.g.*, Z v. Finland, 25 E.H.R.R. 371, 1998, 1997 WL 1104215 (CLC) (Eur. Ct. H.R., Feb. 25, 1997) (holding that it is permissible to gain access to medical records and compel physicians' testimony if necessary in a criminal case. However, it is not permissible to disclose or publish details of that information in such a way that identifies the individual.). *Id. See also* MS v. Sweden, 28 E.H.R.R. 313, 1999, *available in* 1997 WL 1104641 (CLC) (Eur. Ct. H.R., Aug. 27, 1997) (holding that it was appropriate for the Social Insurance Office (SIO) to compel medical record disclosures from a clinic and acknowledging that the clinic, had it not surrendered the records, would be subject to possible criminal and civil liability). However, the court also held that MS's application for insurance compensation did not waive her privacy right in the data and that that SIO's disclosure of the data to other parties was improper. *Id.*

193. *See, e.g.*, Runnymede Community Charge Registration Officer v. Data Protection Registrar, 30 R.V.R. 236, 1990, *available in* 1990 WL 756100 (Data Protection Tribunal, 1990) (clarifying that the Data Protection Act of 1984 applies to data held by the given community agencies, and that those offices could not hold unnecessary information on individuals or their residences based solely on the concern that the data may be necessary in the future). The Tribunal stated that information regarding a person's residence is indeed personal data, and the determination of whether or not this type of data is covered by the Act is one for the Data Protection Registrar to make. *Id. See also* DPP v. Bignall, 1 Cr. App. R. 1, 1998, *available in* 1997 WL 1016155 (CLC) (Q.B., May 16, 1997) (noting that police officers' misuse of data by retrieving information from the police database for personal purposes should be prosecuted under the Data Protection Act, not the Computer Mis-

tional boundaries and span more than ten years, illustrate what appears to be both consistent and reasonable applications of data protection and privacy law.

This is not to say, however, that data privacy laws were not criticized within Europe. The potential commercial impact of the Directive has not escaped notice amongst business and financial writers.[194] For example, normal business relationships, such as those between merged companies, may be disrupted because the two cannot easily share the personal information contained in their respective databases.[195] Additionally, because paper records are also implicated in the Directive, companies may encounter great expense in auditing and managing those paper records to ensure that they are complying with the law.[196] However, European direct marketers, one of the groups most dramatically affected by the rules, appear to have a relatively moderate view of the changes.[197]

They considered early iterations of the Directive to be unworkable, but subsequent changes in the rules, coupled with an improved relationship between the European Commission and commercial groups, significantly softened the marketing industry's attitude.[198] This partnership

---

use Act 1990. The Computer Misuse Act was designed to prohibit hackers from gaining unauthorized access to data, while the Data Protection Act governs the unauthorized use of data. Here, the police officers legitimately had access to the police database, but they were limited to using the data for official police purposes. The use, not the access, was unauthorized).

194. *See, e.g.,* Simon Fluendy, *Privacy Laws may Hit on Lloyds Merger*, Mail on Sunday 52, Oct. 3, 1999; *see also* Reed, *supra* note 17.

195. *See* Fluendy, *supra* note 193. In regards to a pending merger between two companies, Lloyds TSB and Scottish Widows, the article quotes Barrister Andrew Rigby, who is concerned that the Act will require Widows to contact its 1.6 million customers to get permission for Lloyds to directly access each person's data. *Id.* However, if the two companies decide to keep their database separate, Lloyds can have Widows send marketing literature on their behalf. *Id.* While this is more expensive and less efficient than Lloyds contacting the individuals themselves, the strategy would comply with the Directive. *Id.*

196. *See Legal and Financial: Firms Face Huge Paper Chase over New Data Protection Rules*, *supra* note 16. This article reflects some of the more negative reactions of business people to the rules and focuses on the concern that businesses are not sufficiently aware of the Directive and its impact, particularly regarding the massive amount of work involved in managing paper records. *Id.*

197. *See* Reed, *supra* note 17. A review of the Data Protection Act and new Directive reveals concerns in the direct marketing industry over the legislation. However, the article also notes positive changes in the E.U.'s approach to the legislative drafting process and seems to reflect an overall attitude that the data protection rules, while awkward, are workable.

198. *See id.* While the original version of the Directive was "draconian," the process of forcing the Commission to revisit the more restrictive elements led to a number of positive changes. *Id.* For example, the European Commission now works in closer partnership with business interests when developing new rules, the direct marketing industry became

between E.U. government and business may well prove to be a more effective way to produce the type of consistent data protection that the U.S. has so far been unable to achieve.

IV. CONCLUSION

With the advances in technological intrusions, the advent of the unified European market, and approach of the Data Protection Directive, the U.S. must develop a consistent and comprehensive data privacy policy. Even if the U.S. compromises with the E.U. regarding what constitutes "adequate" privacy protections, other countries are moving to adopt the European standards outright.[199] Each country that adopts the E.U. approach potentially puts the U.S. in a position where it will have to suffer the same trade threats and protracted negotiations it is currently enduring with the E.U.[200] International issues aside, the U.S. also faces forces from within that are pushing for increased protections.[201] Up to this point, the U.S. Constitution, federal statutes, common-law precedent, and corporate self-regulation have failed to provide adequate protection for personal data.[202] The various suggestions for shoring up these inadequacies short of legislative action are equally limited and introduce unique judicial problems of their own.[203]

Given the extent of the problems, the U.S. should move quickly towards a legislative solution to resolve the data protection issues facing the nation.[204] This approach would eliminate Constitutional privacy debates, streamline the current jumble of U.S. data protection acts, and

---

more unified, and additional Acts have been created to protect commercial marketing activities. *Id.*

199. *See* Reidenberg, *supra* note 99, at 786-87.

> Even with the difficulties of the European approach, countries elsewhere are looking at the European Directive as the basic model for information privacy, and significant legislative movements toward European-style data protection exist in Canada, South America, and Eastern Europe. This movement can be attributed partly to the pressure from Europe arising from scrutiny of the adequacy of foreign privacy rights, but is also and partly due to the conceptual appeal of a comprehensive set of data protection standards. In effect, Europe has displaced the United States in setting the global privacy agenda with the enactment of the data privacy directive.

Id.

200. *See id.*

201. *See* Kirchner, *supra* note 62. *See also* Sarbanes, 145 CONG. REC. S554-01, S615, *supra* note 54.

202. *See* Cody, *supra* note 96.

203. *See City & Commercial: Bridging the Transatlantic Data Divide*, *supra* note 168.

204. *See, e.g.*, Reidenberg, *supra* note 99. Given the length of time it would take to develop comprehensive data protection law that is acceptable to industry, government, and the public alike, speed is of the essence. *Id.* ". . .[T]he process to enact data protection law in Europe shows that adoption of legal rights is exceedingly slow." *Id.* "The existing European data protection directive took five years and transposition into national law was

harmonize subsequent common law decisions. It would also give the business community clear guidelines regarding its legal responsibility to customers and level the competitive playing field.[205] Companies that adopt and abide by the "safe harbor" principles, for example, have few means to protect themselves from the competitive advantage of companies that choose to violate the principles.[206] Based on the positive example of cooperation between business and government in the E.U., a legislative solution is clearly feasible.[207] However, since this approach cannot provide a solution in time for the enactment of the E.U. Directive, a stop-gap measure is indeed required. Affirmatively linking an authoritative body to the proposed "safe harbor" principles may propel an interim solution. The new Chief Counselor for Privacy, if given the appropriate arbitration, disciplinary powers, and staff, would be a suitable candidate. In fact, the very process of developing such a body would provide valuable insight to the subsequent legislative drafting effort.

Regardless of the course the U.S. ultimately chooses in order to address these problems, there is little doubt that it cannot continue on its current path.[208] A vast legal chasm will be created if U.S. companies are compelled to protect E.U. personal data at a significantly higher level than U.S. personal data. While the double standard might be legal, it makes for exceptionally poor public policy.

---

scheduled for three additional years." *Id.* "In Internet time, these delays are generational." *Id.* at 787.

205. *See, e.g.*, Filetech v. France Telecom, 157 F.3d 922 (1998). When one company manages to take advantage of loopholes in the confusing array of U.S. law, just as Filetech has attempted to take advantage of a disparity between U.S. and European data protection rules, more scrupulous (or less imaginative) competitors are at an inherent disadvantage.

206. *See, e.g., Oversight Hearing on Electronic Communications, supra* note 157. With no investigative or enforcement elements, the safe harbor principles rely on the integrity of individual companies to abide by their promises. *Id.* Unfortunately, the greatest threat to data privacy comes from less ethical companies that have little to fear in the way of repercussions for violating the principles. *Id.*

207. *See* Reed, *supra* note 17.

208. *See* Jake Kirchner, *Your Identity Will Be Digital: Protecting Users' Privacy of Information in a Digital Age*, PC MAG., June 22, 1999.

> As we head into the new millennium, privacy is no longer, in the famous words of Justice Louis Brandeis, the right of every American 'to be let alone.' It isn't even the ability to withhold personal information. How many would forego a home mortgage rather than fill out a loan application? How many would refuse medical treatment rather than divulge their Social Security numbers to insurance providers?
>
> In truth, our privacy hasn't been taken from us. We've bartered it away, bit by bit, for services and modern conveniences. Privacy is no longer about voluntary anonymity. Privacy in the digital age means the ability, through legal and technical means, to control information about ourselves. Equally important will be the widespread social acceptance – even the expectation – of individuals having access to those controls and using them on a regular basis.

Id.

The U.S. must take more pro-active steps to develop a stronger set of data protection rules that are both consistent and easy to apply, whether they are developed through the legislature or through the courts. Given the problems of mixing policy and precedent, however, the most likely solution is a legislative one - one, perhaps, such as the E.U. Data Protection Directive.

Marie Clear