Vanderbilt Law Review

Volume 56 | Issue 3 Article 5

4-2003

The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States

David R. Nijhawan

Follow this and additional works at: https://scholarship.law.vanderbilt.edu/vlr

 Part of the Privacy Law Commons

Recommended Citation

David R. Nijhawan, The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States, 56 *Vanderbilt Law Review* 939 (2019)
Available at: https://scholarship.law.vanderbilt.edu/vlr/vol56/iss3/5

This Note is brought to you for free and open access by Scholarship@Vanderbilt Law. It has been accepted for inclusion in Vanderbilt Law Review by an authorized editor of Scholarship@Vanderbilt Law. For more information, please contact mark.j.williams@vanderbilt.edu.

The Emperor Has No Clothes[1]: A Critique of Applying the European Union Approach to Privacy Regulation in the United States

1. The Emperor Has No Clothes is derived from Hans Christian Andersen's "The Emperor's New Clothes." HANS CHRISTIAN ANDERSEN, THE EMPEROR'S NEW CLOTHES (Naomi Lewis trans., Candlewick Press 1997) (1837). The story involves an emperor who "loved [his] fine clothes more than anything else in the world." *Id.* at 1. Two suspicious characters arrived in the emperor's city and, presenting themselves as weavers, claimed that the cloth they used bore magical properties. *Id.* at 2. According to these weavers, the cloth was invisible to unintelligent people and to people unfit for their jobs. *Id.* The emperor, recognizing an opportunity to see whether his people were fit for their positions, hired the weavers to make him a new set of clothes. *Id.* As one may predict, no one could see the clothes when they were finished. *Id.* at 5. The emperor, his closest aides, and the people, however, all pretended to see these "charming" garments for fear of being labelled unintelligent or unfit for their jobs. *Id.* At the story's climax, as the emperor walks through town in his new clothes, a child mutters that the emperor has no clothes. *Id.* at 13. Soon, everyone else murmurs that he has no clothes and the emperor wondered if they were right, as he was afraid to admit that he could not see the clothes himself. *Id.* at 14. The emperor said to himself, "If I stop, it will spoil the procession. And that would never do." *Id.* As a result, prouder than ever, he walked on through the town, ignorant of his folly. *Id.*

Likewise, U.S. privacy advocates see the EU Directive 95/46 as a new set of clothes, so to speak, for the rights of consumers in the U.S. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) [hereinafter Directive]. These advocates, along with the Directive's weavers, view this as the pinnacle of data protection and believe that it represents the high-water mark of a privacy friendly world where consumers are "respected" on-line. Many U.S. privacy advocates pusb for a similar system in the U.S.

I. INTRODUCTION

Internet users in the United States and the European Union ("EU") often debate the state of international data privacy, while scholars and companies also present questions to the Internet community regarding the regulation of data privacy and the amount of regulation required in the U.S. Inquiries range from how to determine the necessary degree of regulation and how to implement regulations to how to enforce any regulations that the U.S. lawmakers[2] may pass. Historically, the EU and the U.S. approach data[3] privacy regulations in diametrically opposed ways.[4] While the EU relies primarily on

2. Data privacy regulations can come from many different sources. *See, e.g., infra* Part IV.B.3 (discussing Safe Harbor provisions promulgated by tbe Federal Trade Commission ("FTC")). In addition, Congress can pass federal legislation (like the Directive), and states can enact legislation. This Note discusses data privacy rules and regulations at a holistic level in the U.S., regardless of what agency or lawmaking body proposes them.

3. Data collected often include names, addresses, E-mail addresses, etc., which are used to create consumer profiles to aid in marketing efforts.

4. The EU promises strict enforcement of data "rights," while the U.S. has adopted a laissez-faire approach. *Compare* Jennifer E. O'Brien et al., *European Privacy Direetive: A Primer*, PA. BAR ASS'N Q., Apr. 2001, at 84 (noting the EU's strict, legislative approach to data protection), *with* Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH L.J. 357 (2000) (discussing American Internet privacy: "You already have zero privacy, get over it") (quoting Scott McNealy, CEO of Sun Microsystems). *See generally* James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMM. LAW CONSPECTUS 149-50 (2001) (describing the market-based approach). Glancy contends that

legislation and heavy regulation, the U.S. has adopted a market-based, self-regulatory approach to data privacy.[5] The EU further distinguishes itself from the U.S. by implementing an approach that guarantees its citizens protection of their "fundamental rights."[6] Such protection allows for strict governmental control of information flow. The U.S., on the other hand, does not recognize data privacy as a fundamental right, employing instead a less prophylactic approach than that taken by the EU.[7]

Despite these ideological differences, the EU codified its "fundamental right" principle in 1998 when it enacted Directive 95/46 (the "Directive"). With the Directive, the EU created a broad, overarching piece of legislation that gives significant power to the individual with regard to use of her personal information. First, it purports to create uniformity in EU data practices by requiring companies to inform consumers of what they plan to do with the personal information which they collect from their websites.[8] Second, in so doing, the Directive requires the respective companies to secure affirmative consent from consumers to collect, use, and disseminate

---

the U.S. utilizes self-regulation and that consumers do not have privacy rights in the sense that Europeans define privacy. Glancy, *supra*, at 357.

5. *See* Kenneth Mullen, *Data Transfers: Navigating to a Safe Harbor*, CYBERSPACE LAW., July/Aug. 2001, at 8 (noting that the EU takes an interventionist approach, while the U.S. employs a self-regulation approach).

6. Assey & Eleftheriou, *supra* note 4, at 148-49 (discussing the concept of "fundamental rights" and describing the types of controls the government may impose on companies and individuals).

7. The U.S. focuses less on preventive measures and typically gauges market demand and industry self-regulation to determine appropriate levels of privacy on-line. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 64 (2000). The U.S. addresses problems because of supposed "bad-faith" data practices. The Doubleclick litigation is illustrative of this principle. At the time, the U.S. did not have any preventive measures in place like the EU does, and any recourse was after the fact. *In re* Doubleclick, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). Preventive legislation like the EU Directive does not fit squarely with the norm of self-regulation utilized in the U.S.

The EU adopts the principle that privacy is a fundamental right inherent to humans. *See* Assey & Eleftheriou, *supra* note 4, at 145, 148, 150 (noting that the EU considers data privacy as a fundamental and political right and that the U.S. system relies more on social norms, the marketplace, and codes of conduct to protect privacy); Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 879-81 (2000) (arguing that five principles constitute the foundation of U.S. privacy law: a history of balancing competing interests, respect for open flows of information, a desire to be free of government intrusions, a requirement of specific harm and a preference for self-help measures); *see also* Directive, *supra* note 1, art. 1, para. 1 ("Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.").

8. *See, e.g.*, *infra* notes 74-75 and accompanying text; *see* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 191 (1999).

this information.[9] Third, once companies obtain consent, they must document and register the consent with local "data authorities" who retain the information in their own databases.[10] Fourth, during this process, the Directive allows individuals to access their information and allows them to request amendments and/or corrections to their data.[11] Finally, the Directive also allows individuals to know the identity of the companies collecting their data.[12] Assuming that the company uses the information consistent with its stated purpose, the Directive then requires the company to relinquish information that has already been used.[13] In the international context, the Directive explicitly bars data transfers to other countries that do not provide "adequate" data protection, as defined by the Directive.[14]

In promulgating the Directive, the EU broadened the distinction between the U.S. and EU approaches to Internet privacy, ultimately presenting global companies with a conundrum concerning the appropriate method to use.[15] The competing U.S. and EU

---

9. *See* Omar Saleem, *The Establishment of a U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and Its Impact on U.S.-China Relations: Marco Polo Where Are You?*, 19 J. MARSHALL J. COMPUTER & INFO. L. 169, 179 (2000); *infra* notes 79, 85 and accompanying text. However, the EU system, while identifying "consent" as a de facto requirement, appears to create exceptions, or at least inconsistencies, with that requirement. For example, to my knowledge, machines like European automatic teller machines take pictures of customers (thereby, presumably falling under the ambit of "personally identifiable information"), but do so without "asking" every single person on every occasion if they consent to this type of intrusion. This serves to make the Directive even more complex and, in the end, unworkable.

10. *See* Bruce E.H. Johnson, *The Battle over Internet Privacy and the First Amendment*, 18 No. 4 COMPUTER & INTERNET LAW., Apr. 2001, at 21-22; *see also infra* notes 82-83 and accompanying text. *See generally* Directive, *supra* note 1.

11. *See generally* Directive, *supra* note 1, art. 12(a); Cate, *supra* note 8, at 183-84; *infra* note 81 and accompanying text.

12. *See* Alain Bensoussan, *Data Protection: EU Directive and Safe Harbor Principles*, PLI/PAT 291, 296 (2001).

13. Cate, *supra* note 8, at 182 n.48; *infra* notes 82, 86 and accompanying text. In the international context, the Directive also bars, per se, data transfer to other countries that do not provide "adequate" data protection as defined hy the Directive. *See* Directive, *supra* note 1, art. 25(1); *infra* note 84 and accompanying text.

14. *See* Directive, *supra* note 1, art. 25(1). The Directive states that member states must provide "adequate" protection, but falls short of providing a solid, reliable definition of the term.

15. On the one hand, some U.S. companies (or other companies outside the EU) see the Directive as a preventive measure utilized by the EU to protect EU companies from foreign companies entering their market. Thus, some of those companies undoubtedly contemplate the value of adhering to every provision. On the other hand, many companies recognize that compliance imposes serious transaction costs and destroys a significant part of the business model in some cases. *See* Stephen Baker et al., *Europe's Privacy Cops*, BUS. WK., Nov. 2, 1998, at 49, 51; Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 143-44 (2000); *infra* notes 44, 48 and accompanying text. As a result, companies have a difficult choice to make. *See* Assey & Eleftheriou, *supra* note 4, at 146-47 (discussing the precarious situation businesses find themselves in when complying with the Directive). The EU approach gives citizens a variety of

ideologies create a unique yet frustrating problem for Internet companies around the world,[16] including both brick-and-mortar stores as well as "virtual" companies.[17] Business globalization, together with e-business growth, creates situations in which one country's laws may have substantial effects upon those of another country.[18]

This Note focuses on the Directive's effect on the United States. This Note argues that implementing a similar omnibus system in the U.S. is not feasible.[19] The Directive is a façade rather than an actual, workable solution to privacy concerns. Although some scholars offer significant policy arguments in favor of implementing more regulation in the U.S., the inquiry should be limited to whether the U.S. really needs stricter privacy regulations and, more importantly, whether the U.S. legal framework places constraints on implementing such broad legislation instead of self-regulation. U.S. policymakers should strive to find a workable, reasonable solution that fits within the constructs of existing values and norms in the privacy arena rather than institute an extremely rigid and an unworkable solution. From a practical standpoint, this Note also contends that the EU Directive 95/46, from a practical standpoint, is not a feasible solution for the U.S. Further, the Directive is not what it purports to be, because the Directive is not as uniform as its proponents claim, nor does the EU strictly enforce it. Ultimately, EU and U.S. privacy advocates who encourage similar legislation in the U.S. appear naked without their clothes much like the ill-fated emperor—because they encourage legislation that will never function in reality.

Prior to analyzing this question, it will be helpful to understand its relevance. Therefore, Part II of this Note provides

---

rights. EU citizens maintain the right to special information such as the identity of the person who controls their information in addition to information regarding the reasons why companies are processing their information. *See generally* Directive, *supra* note 1, art. 10. Further, the EU affords its citizens the right to know who receives their data, and it also affords them the right to amend the data should they so desire. *See* Bensoussan, *supra* note 12, at 296 nn.7-10.

16. Outside companies face the possibility of the EU barring them from trading in the EU if they do not comply with the Directive. Companies forced into this frustrating situation must weigh the costs of compliance against the costs of not doing business in the EU. This dilemma creates a precarious situation for companies developing a long-term value strategy.

17. "Virtual companies" refer to purely E-commerce vendors (those which sell directly and exclusively from the Internet).

18. Joshua S. Bauchner, Note & Comment, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, 26 BROOK. J. INT'L L. 689, 691 (2000).

19. The EU directive affects not only U.S. business, but the U.S. legal system as well. The U.S. has already responded to the EU Directive with the Safe Harbor provisions. *See* discussion *infra* Part IV.B.3. If privacy advocates' suggestions are followed, more legislation will arise in the data privacy context. Following the EU's lead in data privacy protection could hamper the legitimate business interests of U.S. companies. *See id.* (discussing in detail how the EU system effectively encroaches on the sovereignty of other countries).

background to the U.S. and EU systems and outlines faults in the EU system. Part III of this Note focuses on the inherent value of information to companies, and the reasons why data transfer restrictions create considerable problems for on-line companies. In Part IV, this Note details the EU approach to on-line data privacy, the traditional U.S. approach of market-based self-regulation and the Safe Harbor approach. Parts V through VII of this Note address the fact that a true EU-style model will not function properly within the U.S. legal framework. In addition, Parts V, VI, and VII contend that a carbon-copy EU-style model will: (1) interfere with the free flow of information, (2) lack uniformity, and (3) lack appropriate enforcement mechanisms. Finally, in Part VIII, this Note argues that, because of the concerns raised, an EU-style regulation is not a real solution for data privacy concerns in the U.S.

II. BACKGROUND ON THE U.S. AND EU APPROACHES TO DATA PRIVACY

The Directive's introduction prompted U.S. privacy advocates to encourage similar legislation in this country as part of a more active stance toward privacy regulation.[20] Many of these privacy advocates look to the Directive as the "code" to which all companies should conform their privacy practices.[21] Other advocates argue that the current U.S. market-based approach is unsound and ineffective.[22] Finally, some U.S. privacy advocates foresee an EU-style system functioning effectively in the U.S. and conforming to the U.S. legal infrastructure.[23]

As a result of this debate among privacy advocates, the Federal Trade Commission, representing the U.S., negotiated with the EU to create some semblance of compromise.[24] These negotiations produced

---

20. The following organizations have all shown support for an EU-style approach in the U.S.: the Electronic Frontier Foundation (www.eff.org), the Electronic Privacy Information Center (www.epic.org), the American Civil Liberties Union (www.aclu.org), the Global Internet Library Campaign (www.gilc.org), and the Internet Free Expression Alliance (www.ifea.net).

21. *See* Assey & Eleftheriou, *supra* note 4, at 147-48 (noting that the EU directive and the resulting Safe Harhor provisions were considered groundbreaking).

22. *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 787 (1999); Shaffer, *supra* note 6, at 64.

23. *See* Shaffer, *supra* note 6, at 64 (noting the concerns of privacy advocates that the U.S. needs a comprehensive privacy protection approach, as opposed to a "scandal-specific" one); *id.* at 64 n.272 (noting that some advocates call for the use of data authorities like those in the EU); *id.* at 78 (quoting Marc Rotenberg and characterizing the U.S. system of self-regulation as "smoke and mirrors").

24. The Safe Harbor principles arose from years of negotiations between the U.S. and the EU to reconcile these differences. *See* Bauchner, *supra* note 18, at 714; Stefania Geraci,

the "Safe-Harbor" Principles[25] (the "Safe Harbor"), a voluntary set of guidelines under which U.S. companies can certify to consumers[26] that they will follow certain articulated guidelines for Internet privacy. Proponents heralded the Safe Harbor[27] as a means for U.S. companies to conduct business in Europe without adhering to each of the Directive's provisions,[28] because it essentially created a backdoor route for U.S. companies to fulfill the Directive's "adequacy" requirement. [29] Seven fundamental principles comprise the Safe Harbor[30]: (1) notice, (2) choice, (3) onward transfer, (4) security, (5) data integrity, (6) access, and (7) enforcement.[31]

Through the Safe Harbor, the FTC tried to create a quasi-EU regime, while still providing companies with some leverage in utilizing consumer information for marketing purposes.[32] Despite the long negotiations between EU representatives and their U.S. counterparts and their attempts to create a set of regulations that strikes a balance between the two approaches to data privacy, scholars and companies have debated the effectiveness and functionality of the Safe Harbor approach.[33] These debates reflect concerns that joining the Safe Harbor often creates more problems than not joining.[34] Certification

---

Congressional Hearings Focus on Privacy Issues, 18 No. 4 E-COMMERCE L. & STRATEGY 8 (2001) (noting commentators that support regulation by saying a formal and uniform federal standard would be a positive step).

25. Discussion *infra* Part IV.B.3.

26. Companies can elect to certify themselves as a Safe Harbor company. This certification provides notice to consumers that the company agrees to comply with the basic standards set forth in the Safe Harbor provisions. *See* Tamara Loomis, *Data Privacy: A Few Companies Have Complied with the EU Law*, 226 N.Y. L.J. 5, Aug. 30, 2001, at 5 (discussing the Safe Harbor provisions and noting that under Safe Harbor, companies assert that they comply with the basic standards set forth by the EU); *see also* U.S. DEP'T OF COMMERCE, SAFE HARBOR, *at* http://www.export.gov/safeharbor/sh_overview.html, (noting that "[c]ompanies participating in the safe harbor will be deemed adequate and data flows to those companies will continue")

27. *See supra* notes 21, 24 and accompanying text. The Safe Harbor was a direct result of and is a functional equivalent to the Directive.

28. Amee A. Shah, *How Human Resource Administration in a U.S. Company is Affected by the Safe Harbor Directive*, 9 METRO CORP. COUNS., Mar. 2001, *available at* www.westlaw.com.

29. Directive, *supra* note 1, § 25(1). The Directive requires that each member-state provide "adequate" data protection. *Id.*

30. Discussed *infra* Part IV.B.3.

31. U.S. DEP'T OF COMMERCE, SAFE HARBOR, *at* http://www.export.gov/safeharbor/sh_overview.html (last visited Mar. 3, 2003).

32. Shah, *supra* note 28.

33. *Id.*

34. The main problem with this framework is that it can impose additional jurisdictional requirements. When companies certify under the Safe Harbor, they create their own problems by opening themselves to the jurisdiction of the FTC, the EU, and the member states in which they do business. The EU also does not limit its reach to physical stores in their domain. For example, a foreign company that accesses information from an EU country could find itself subject to another country's jurisdiction if the Internet infrastructure routes the information through a

under the Safe Harbor automatically subjects U.S. companies to FTC jurisdiction, along with the jurisdiction of the EU and each member state.[35] Theoretically, the FTC, the EU, or any member state can all raise claims against members of the Safe Harbor.[36] This increased potential for litigation constitutes an obvious disincentive for any company to join the Safe Harbor despite the attempt to retain some flexibility for companies under the Safe Harbor provisions.[37]

Substantial ramifications arise from this disincentive to join the Safe Harbor. Although the Safe Harbor purports to encourage a more respectful on-line environment, the reality is that an insignificant number of U.S. companies certify themselves under the Safe Harbor.[38] Even with industry giants such as Microsoft and Hewlett-Packard certified under the Safe Harbor, the number of U.S. companies currently certified remains small.[39] Consequently, the Safe Harbor's future remains unclear as to whether more companies will join its ranks. This lack of participation creates a problem because certified companies must compete on unequal planes, thereby creating a substantial adverse economic effect on companies and their direct marketing strategies.[40]

However, in the new economy, the access and use of consumer data are invaluable,[41] because many U.S. direct marketing corporations rely on the ability to collect and analyze data for their economic viability.[42] The value proposition[43] for many companies lies

---

third member state. This jurisdictional breadth creates a slippery slope as the next step for the EU or the member states to start would be to impose hardware regulations and various other technical requirements on companies. These changes result in more money spent to comply with provisions that keep changing—which could actually decrease profitability for companies.

35. *See* Henry L. Judy & Benjamin S. Hayes, *Between a Rock and an Unsafe Harbor—Options for Compliance with the EU Data Protection Directive*, ELEC. BANKING L. & COM. REP. 14, Mar. 2001; *infra* note 108 and accompanying text.

36. *Id.*

37. *Id.*

38. U.S. DEP'T OF COMMERCE, SAFE HARBOR LIST, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (providing a list of the 291 companies that have joined the Safe Harbor) (last visited Jan. 24, 2003). While some larger companies like Microsoft have joined the list, the total number of companies remains small in proportion to the overall number of companies that do business on-line.

39. *Id.*

40 *See* Shaffer, *supra* note 7, at 18 ("[B]y impeding businesses from obtaining information, more stringent privacy protection reduces their efficiency. For example, privacy protection makes it more difficult for firms to obtain information about job applicants' past performance.").

41. Joel R. Reidenberg, *E-commerce and Trans-Atlantic Policy*, 38 HOUS. L. REV. 717, 719-20 (Fall 2001); Paul Rose, Comment, *A Market Response to the European Union Directive on Privacy*, 4 UCLA J. INT'L L. & FOREIGN AFF. 445, 449 (1999/2000); *see also* Cate, *supra* note 7, at 881-82 (discussing how companies can use information to better serve customers).

42. In the U.S., direct marketing sales accounted for 1.2 trillion dollars in 1997, and in Europe, only 125 billion dollars. Shaffer, *supra* note 6, at 18-19; *id.* at 18 n.64; *see* Kevin Bloss,

in the fact that consumers allow them to collect, disseminate, and mine[44] their customer information.[45] In some cases, these data are the company's only asset.[46] Thus, the costs of compliance with an EU-style

Raising or Razing the E-curtain?: The EU Directive on the Protection of Personal Data, 9 MINN. J. GLOBAL TRADE 645, 653 (2000) (noting that the U.S. remains the "leading power" in Internet business and that rejecting compromises could prevent EU companies from harnessing the power of the Internet). Further, under the EU system, when companies fail to get the information, operating costs go up. *See* Shaffer, *supra* note 6, at 18 n.62 ("Businesses may still be able to 'get the information they need,' but only 'if they can afford the expense.' ") (quoting Stephen Baker, *Europe's Privacy Cops*, BUS. WK., Nov. 2, 1998, at 20).

43. As defined by an EDS management consultant, a value proposition is: "How value is going to be delivered to a client/prospect, through the execution of some strategy or tactic, and what the expected result is going to be." Telephone Interview with Pradeep Nijhawan, EDS consultant (Feb. 16, 2002).

44. Data mining is the practice of consolidating data into useful formats or useful information that can be used for business purposes. "Data exchange, already a critical issue for business, is a key to marketers' global ambitions. Their plan is to plumb databases of buying patterns, develop thousands of detailed consumer profiles, and then hit buyers with finely tuned pitches—preferably on-line." Baker, *supra* note 15, at 20.

45. Profiling consumers to provide a more customized and interactive shopping experience provides an inherent value proposition of companies like Amazon.com. Similarly, companies like Gap, Inc. track website visits and what items the user bought in the past. After consolidating this information, the company then utilizes active webpages to customize the individual's shopping experience. This practice has been used as a mutual benefit to the business as well as the consumer long before on-line commerce evolved. Grocery stores are a classic example of this type of practice with their "value cards." *See* Singleton, *supra* note 15, at 143-44 (2000). Singleton explores the effects of grocery store data collection practices:

> Assuming human dignity is defined, should all actions that violate human dignity be illegal? How is human dignity offended if Safeway learns through a Safeway card that I am in the habit of buying pineapples and do not own my own home? Our intuitive understanding of human dignity and human rights is probably sufficient to allow us to understand that we ought not to be subject to torture by the police, or to starve prisoners of war. But it does not bring us to the understanding that it is wrong for businesses to collect data about their customers without the customers' consent, especially given the fact that we routinely do this sort of information gathering in our ordinary private lives. While we often desire to conceal facts about ourselves from others, we also at times have an interest in learning information about others. A concept that sees information gathering for the purpose of commerce as an offense to human dignity, must suppose that human dignity is very fragile. Do we really need the federal government to protect us from being embarrassed? Can we assert a right not to be embarrassed? Surely a government interest in protecting human dignity must be founded on something more substantial than vague fears that someone somewhere may obtain information about you and might use that information to try to sell you products, or annoy you with junk mail. And how is it consonant with human dignity to prevent businesses from communicating truthful information about real events to other businesses?

Id. If an EU-style system were implemented in the U.S., the value of direct marketing such as this would likely be minimized.

46. *See* James J. Dillon et al., *Minimize the Risks of Privacy Violations When Operating E-Commerce Web Sites*, N.J. L.J., Sept. 16, 2002. Toysmart, in its privacy policy statement, stated that the information collected would not be sold to any third parties or used by any third parties. *Id.* When Toysmart.com filed for Chapter 11 proceedings, the company attempted to renege silently on this policy by trying to sell the information collected in their database as an asset. *Id.* Privacy groups quickly attempted to stop the selling of the data. *Id.* This case was novel because the information constituted Toysmart's only real asset in their Chapter 11 proceeding.

regime endangers the economic success of many American companies.[47] In addition, a dearth of hard evidence exists that the alleged "abuse" by corporate America adversely affects consumers so as to necessitate broad regulation.[48]

In spite of these concerns, data collection practices constitute the lifeblood of the direct marketing industry in the U.S.[49] Following the EU's lead would therefore essentially put this country one step closer to George Orwell's vision in *1984*, not only from a business perspective, but also from a perspective of greater government influence over personal privacy.[50] This government control would occur because the central provisions of the EU legislation give the government greater control over personal data, despite information privacy being characterized as a fundamental human right.[51] The Directive effectively expands government influence rather than curtails it, which directly conflicts with widely held American values regarding personal privacy.[52] Historically, U.S. citizens distrust the government with their personal information more than they distrust individuals.[53] Consequently, it seems counterintuitive that advocates seek to vest additional power in the government to control their personal data via an EU-style regulatory framework.[54] Implementing an EU-style regulation in the U.S. as a binding provision on companies makes little sense. U.S. companies already face significant

47. *Supra* note 42 and accompanying text.

48. *Infra* note 48 and accompanying text. It appears, however, that privacy advocates attempt to incite emotion and gather support by creating scenarios that do not actually exist.

49. *See, e.g.*, Rose, *supra* note 41, at 449; Reidenberg, *supra* note 41, at 719.

50. In *1984*, Orwell described a social infrastructure in which the government literally had unfettered discretion to monitor individual actors. GEORGE ORWELL, 1984, at 23 (Penguin Books 1999) (1949).

51. *See* Cate, *supra* note 8, at 183-84 (noting that the structure of the Directive gives substantial power to the data authorities (which remain government-sanctioned) over the flow of data). By requiring affirmative consent from each individual, the EU creates a situation in which personal data automatically will be linked to the names of individuals—which contradicts the desire of privacy advocates that names *not* be tied to personal information. *See id.*

52. Traditionally, U.S. citizens have worried more about government abuse of information than about abuse by private actors. *See* Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648 (1995) (noting that privacy advocates support the EU model in the name of individual civil liberties). However, supporting an EU-style model seems inapposite to the idea that the government cannot be trusted and the idea that we want a decentralized government. Essentially, the EU creates a more powerful government. *See* Charles Bogino, *Privacy: EU Commissioner Says Current U.S. Law Inadequate to Protect Financial Services*, INT'L BUS. & FIN. DAILY, May 14, 2001 (noting significant cultural differences). For example, Americans are more concerned with intrusion by the government into their privacy than with individuals' or companies' intrusions. *Id.*

53. *See supra* note 52 and accompanying text.

54. *See* Cate, *supra* note 8, at 220, 225-26.

consequences for joining a nonbinding approach like the Safe Harbor, and implementing such a system like the Directive in the U.S is therefore likely to prove problematic.[55]

III. THE INHERENT VALUE OF INFORMATION

Information possesses inherent value for companies. In the digital age, companies collect and process massive amounts of information in previously unavailable ways,[56] as the Internet makes the collection of personal information much easier via cookies,[57] click stream data,[58] on-line surveys,[59] and registration forms,[60] in addition to other data collection tools. As a result, companies can collect information in a quicker, more efficient, and less expensive manner.[61]

---

55. By certifying under the Safe Harbor provisions, companies subject themselves to new jurisdictions that did not exist previously. *Cf.* Judy & Hayes, *supra* note 35. This consequence does not provide any incentives for companies to join because it subjects U.S. companies to the jurisdiction of the FTC. *Id.* Additionally, it subjects U.S. companies to higher scrutiny than current U.S. laws even when they are in U.S. courts. *Id.* Further, companies incur extraordinary costs of compliance when adhering to the EU Directive or joining the Safe Harbor. *Id.*

56. *See* Erin M. Egan, *Internet Privacy*, ALI-ABA COURSE OF STUDY, MAR. 22, 2001, at 527, 529; *infra* note 61 and accompanying text (noting that information is collected in unprecedented ways on a worldwide level).

57. Companies use cookies (among other tools) to collect data from consumers. *See* Anna Shimanek, *Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455, 457, 460-61 (2001) (providing an excellent discussion of different business methods companies use to collect information (including cookies, clickstream data, etc.)); SEARCHSECURITY.COM,DEFINITIONS:COOKIE, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211838,00.html (last visited Jan. 21, 2003):

> A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time. (More technically, it is information for future use that is stored by the server on the client side of a client/server communication.) Typically, a cookie records your preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests.

58. *See* SEARCHSYSTEMSMANAGEMENT.COM ("In Web advertising, a click stream is the sequence of clicks or pages requested as a visitor explores a Web site.") (quoting from "whatis.com" website search), *at* http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci211794,00.html (last visited Mar. 3, 2002).

59. *See* Shimanek, *supra* note 57, at 460-61.

60. *Id.*

61. *See* Egan, *Internet Privacy*, *supra* note 56, at 529 (noting that the Internet bas dramatically improved "the ability of companies to gather personal information"). Websites and computer technology make it quite easy for one to "collect, reproduce, disseminate, and compile" individual information. Ruth Hill Bro, *Privacy and Data Protection in the Business-to-Business Context*, *in* SOLVING THE LEGAL ISSUES AFFECTING B2B TRANSACTIONS, at 321, 323 (Patents, Copyrights, Trademarks, & Literary Prop. Course Handbook Series PLI Order No. 60-00NF, 2001). For example, companies can use forms, E-mails, cookies, and other tools. *Id.* Further, website payment systems often collect details about the parties to the transaction, as well as

This information collection provides invaluable benefits to both Internet companies and brick-and-mortar companies[62] due to the high premium for information on the open market. In other words, the essence of effective business in the information economy is in efficient information control practices.[63] Timely, refined customer information gives companies a strategic advantage in the virtual marketplace because it provides companies with a powerful weapon over competitors in developing marketing strategies.[64] In fact, the future of an on-line business depends on its ability to secure information.[65] As one commentator has noted:

> Companies engaging in electronic commerce have a significant interest in personal data, and its transfer online. Transborder data flow bas become indispensable to the very existence of transnational enterprise and to the currently flourishing global marketplace.... [I]nformation is the *lifeblood* that sustains political, social, and business decisions. [66]

Quality information control practices remain pivotal to customer service. For example, information gathering gives companies the ability to target products and advertisements specifically to their customers.[67] Additionally, free-flowing information allows companies

---

details about the transactions themselves. As companies share this information with affiliates, large databases of information are built. *See* Reidenberg, *supra* note 65, at 720 ("E-commerce leaves an extensive trail of personal information. Internet service providers and Web sites log user interactions for technical and commercial operations."); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1126 & n.2 (2000) ("The technical infrastructure of cyberspace makes it remarkably simple and inexpensive to collect substantial amounts of information identifiable to particular individuals.") (citing Cate and Kang articles).

62. *See infra* note 65 and accompanying text (noting that information is the lifeblood of the on-line industry).

63. *See* Rose, *supra* note 41, at 449 (noting that on-line companies profit greatly from these data collection practices). As a primary business, several companies track consumer data and collect this information for business and marketing purposes. Some examples include "Engage Technologies, Acxiom, DoubleClick, and Clickstream." *Id.*; *see also* Shimanek, *supra* note 57, at 457 n.9 (noting that consumer companies consider databases to be an intangible asset in the marketplace since they use them to create targeted advertisements and develop marketing strategies).

64. *Id.*

65. "Online commercial transactions depend on both the creation and availability of unprecedented and extensive data about individuals." Reidenberg, *supra* note 41, at 719-20.

66. Bauchner, *supra* note 18, at 709 (emphasis added) (quoting Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 989 (1991)).

67. This type of information freedom remains fundamental to a market economy. Consumer needs are reflected in a desire to have products delivered on time and to have their further needs predicted by companies. Companies satiate these needs, in part, by collecting and disseminating this information so that the needs are met in real time. Ultimately, these practices are enabling, not only for companies, but for consumers as well—the question, or the issue, must be framed in the appropriate manner. Cate, *supra* note 7, at 881-82. "The ready availability of public record 'data facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want.' " *Id.* at 884 (quoting FRED H. CATE & RICHARD

to profile its customers more effectively in order to provide the goods and services that consumers want.[68] All of these benefits keep the direct marketing industry alive. As noted above, however, while the marketplace places a high value on information, the EU and the U.S. take very different paths in the procurement, propagation, and most importantly, the protection of personal information collected on the Internet.[69]

IV. FRAMEWORK OF THE EU AND U.S. MODELS FOR DATA PROTECTION

A. The EU Approach

The EU approaches data privacy in a much more robust fashion than its U.S. counterpart.[70] Instead of relying on social norms or on a market-based laissez-faire system, the EU enacted broad legislation and promulgated regulations that significantly affect data flow across national borders.[71] Unfortunately for its U.S. counterpart,[72] the EU regulations impose stricter standards than the morals of the marketplace. Ultimately, the EU system rests on the foundation that information privacy is a fundamental human right,[73] and it also allows individuals to control the way in which companies collect and use their information. As one commentator noted:

> The EU Directive recognizes privacy as a fundamental human right. The EU Directive's guidelines for information privacy are: personal data is collected for specific legitimate purposes; the data must be relevant, accurate, current, not excessive and kept no longer than necessary; personal data may be processed only if the Internet user has unambiguously given consent (or under specified exceptions); member states must establish supervisory bodies, (e.g., commissions, regulatory agencies) and remedies for a

---

J. VARN, THE PUBLIC RECORD: INFORMATION PRIVACY AND ACCESS—A NEW FRAMEWORK FOR FINDING THE BALANCE 10 (1999)).

68. *Id.* at 881-82.

69. *Supra* notes 4-8 and accompanying text.

70. *See* Jonatban M. Winer, *If the US is From Mars and the EU is From Venus, What Do You Do in Cyberspace?*, PRIVACY & INFO. L. REP., Apr. 2001 (noting that the EU takes a much broader approach in that "if it moves, we regulate it" and that the U.S. takes a self-regulation approach).

71. *See* Bloss, *supra* note 42, at 650-51 (noting that the U.S., not the EU, uses a laissez-faire system predicated on self-regulation).

72. The term "counterpart" refers to U.S. lawmaking bodies in general. For purposes of this discussion, privacy regulations can come from the FTC, Congress, state legislatures or agencies, or any other lawmaking body.

73. *See* Samuelson, *supra* note 61, at 1170 (noting that Europeans "have identified information privacy as a fundamental value that should be a keystone of the architecture for achieving an information society in which people will want to live"). Pamela Samuelson offers the proposition that a large part of the problem might be that no clarity exists as to how U.S. citizens actually value their on-line privacy. She does note, however, that a lack of proper definition of the nature of interest involved is a large part of the problem. *Id.* at 1170-71.

> breach of privacy rights; and, transfer of data to a third country is restricted unless the third country has an adequate level of protection for data privacy [74]

At a conceptual level, Europeans are traditionally more apprehensive about free transfer of personal information to companies or other individuals.[75] Accordingly, the EU uses a prophylactic approach with regard to abuse of personal information.[76] As part of this approach, the Directive provides exacting standards that the member states and companies must meet before companies in those states can collect and use personal information from EU citizens.[77] It requires: 1) that personal ownership of information and consent to use this information be shown, 2) that the information be used for its specified purposes, and 3) that companies provide an "adequate" level of protection.

1. Personal Ownership and Consent

The Directive provides for personal ownership of data, individual access rights to data from data controllers, and individual consent to the use of personal data.[78] Member state laws must allow data subjects to "correct, erase or block the transfer of inaccurate or incomplete data," and they must allow for the erasure of personal data without cost.[79] The Directive requires that companies use personal information only for "specific and clearly stated purposes" when

---

74. Saleem, *supra* note 8, at 177; *see also* Barbara Crutchfield George, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply With the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 742-43 (2001) (noting that EU legislators based the EU's data privacy laws upon this fundmental right).

75. George, *supra* note 74, at 743; *see id.* at 741 n.23, 744-45 (providing a discussion on the evolution of European data privacy laws and noting that the Spanish Constitution includes privacy rights, while similar UK legislation acknowledges the "right to respect" for individuals' private lives); Reidenberg, *supra* note 41, at 731 (noting that in the EU, "citizens trust government more than the private sector with personal information").

76. Winer, *supra* note 70. Advocates view the Directive as more protective of privacy rights than U.S. laws and regulations. *Id.* This is because the EU recognizes privacy as a fundamental right, and the EU requires that national laws exist with regard to Internet privacy. *See* Saleem, *supra* note 8, at 177.

77. *See generally* Directive, *supra* note 1.

78. *Id.* art. 12(a). Generally, a data controller is the person or company that is collecting information from the customer on the Internet—the EU grants the consumer access rights to this information and also allows the customer to receive confirmation that his information is only being used in ways approved by her. Privacy advocates also refer to this as "information self-determination." TERRY R. BRODERICK, REGULATION OF INFORMATION TECHNOLOGY IN THE EUROPEAN UNION 73-74 (2000) (noting that Article 12(a) provides a data subject with rights to confirmation of whether data relating to her is being processed); *see, e.g.*, Cate, *supra* note 8, at 183 (discussing the Directive's mechanics with regard to information access and use in the EU); Reidenberg, *supra* note 22, at 782 n.52; *see id.* at 183 n.52.

80. Cate, *supra* note 8, at 183.

conducting business in the EU.[80] It further mandates that companies obtain individual consent before information may be collected.[81] The Directive requires that companies must not only obtain consent from each individual, but also that they verify this consent with a data authority[82] before processing the information. Once a company collects personal information, the Directive imposes additional constraints on the use of this information and the length of time a company may retain this information.[83]

2. Data Can Be Used Only for Specified Purposes

The Directive imposes additional controls by requiring that companies use data for only those purposes that the business previously identified.[84] Ultimately, the specific use requirements of the Directive impose stricter data controls on data transfer than those currently applied in the U.S. While this does not pose a significant problem within the EU, it creates substantial problems in the international context, particularly in information transfers between the EU and the U.S., because any collected information must be destroyed immediately after its use. This practice deprives companies of valuable information and causes tensions in the international context when one analyzes the "adequacy" requirement.

3. The Adequacy Requirement

The Directive states that countries outside of the EU must provide an "adequate" level of protection before they can collect and

---

80. Keith Perine, *How Private is Private Enough?*, INDUSTRY STANDARD, Feb. 28, 2000, *available at* 2000 WL 31584579.

81. Cate, *supra* note 8, at 191. The Directive also provides a catch-all by stating that the individual should be able to "opt-out" (for direct marketing purposes) at any time. *Id.* at 191 n.88.

82. *See infra* notes 167-169 and accompanying text (noting that as a surrogate of the government, data authorities (supervisory authorities) retain the authority to investigate data processing between companies and individuals. The Directive grants them access rights to the information. Data authorities also serve the purpose of documenting consent from individuals and storing that information. Finally, the Directive grants them the power to interfere with the flow of information if companies violate member state law(s)).

83. Cate, *supra* note 8, at 182.

84. The Directive grants "European citizens absolute control over data concerning them. If a company wants personal information, it must get that person's permission and explain for what purposes the information will be used. It must also promise not to use it for anything else without the citizen's consent." Baker et al., *supra* note 15, at 20; *see also* Bruce C. Doeg & Jason Epstein, *Small Small World: Even U.S.-Focused Web Sites Can Trigger Global Legal Concerns*, LEGAL TIMES, June 4, 2001 (noting that the Directive provides protections that allow "collecting data only for 'specified, explicit, and legitimate purposes' " and for obtaining consent); *Cf.* Winer, *supra* note 76 (noting that personal information must be destroyed when it is no longer needed).

disseminate information gathered from EU citizens.[85] The Directive does not, however, provide a bright-line definition of "adequate." Because the term is open to extensive interpretation, the Directive ultimately forces companies to attempt to conform their behavior to a highly subjective standard.

The Directive grants member states a certain amount of autonomy in deciding what level of privacy protections they may invoke to meet the adequacy requirement. Provided that the protections remain at a level at least equal to the minimum requirements of the Directive,[86] member states remain free to institute policies and regulations that are more demanding than those required by the Directive.[87] At least in theory, the Directive's adequacy requirement creates the potential for ten to fifteen independent data privacy policies within the EU, rather than a single cohesive piece of legislation.[88]

B. The U.S. Approach

Reconciliation between the EU and the U.S. approaches to privacy regulation remains difficult because of their contrasting core values regarding personal privacy over the Internet.[89] Both the EU

---

85. The Directive explains the assessment of whether a third country offers an "adequate" level of protection:

> 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.

Directive, *supra* note 1, art. 25(2).

86. Bensoussan, *supra* note 12, at 294; *see* Cate, *supra* note 8, at 185 (noting that the Directive imposes only *minimum* protections and that each member state can adopt more stringent policies).

87. *See* Bensoussan, *supra* note 12, at 296 (noting that the Directive gives data subjects the right to certain information, and that they retain the right to know the identity of the controller and her representative, "as well as, information regarding the purposes of the processing of the data"); *see* Reidenberg, *supra* note 41, at 733 n.100 (noting the Directive grants member states authority to enact their own independent, national supervisory authority to enforce their privacy provisions) (citing the Directive, *supra* note 1, art. 28(1)).

88. The possible number of different privacy regulations depends on the number of member states.

89. *See* George, *supra* note 74, at 741 (noting the tension created as a result of differing cultural and legal attitudes between the U.S. and the EU). Though this specific instance referred to data privacy practices in the employment context, the same general principle applies in the EU outside of the workplace context. *Id.*

See Cate, *supra* note 8, at 179 (noting that U.S. and EU core values conflict and that laws and legal regimes from one country affect other countries because of the global nature of data);

and the U.S. recognize the privacy needs of consumers. The U.S. system, however, balances personal privacy interests against the competing legitimate economic interest in collecting and utilizing public information for business purposes.[90]

Unlike the EU, the U.S. adopts a self-regulatory approach to Internet privacy regulation, dictated by the morals of the marketplace.[91] Grounded primarily in industry norms and industry reactions to market pressures, the U.S. has not adopted the same broad, prophylactic rule[92]. Generally, the U.S. prefers less government interference with privacy rights and prefers less overarching legislation.[93] Because U.S. history indictates a disdain for broad, omnibus data privacy legislation, this country arguably views overarching legislation as the least-preferred method in most situations.[94] Therefore, privacy advocates clash with the industry leaders who argue that larger government influence is inapposite to

---

cf. George, *supra* note 74, at 741-50 (noting the clash of privacy values between the U.S. and the EU).

Professor Cate also notes: "If a regulatory approach is to be pursued, then global standards are necessary. But the conflict between the core values of the European and U.S. systems of privacy protection makes global consensus on effective privacy standards little more than a mirage." Cate, *supra* note 8, at 228; *see also* Saleem, *supra* note 9, at 178 (noting that the differing practices of the EU and the U.S. with regard to Internet privacy reflect the legal and cultural differences between the two entities).

90. *See* Bloss, *supra* note 42, at 650-51 (arguing that the U.S. approach creates economic advantages in the marketplace). This paradigm has yet to take hold in Europe, thus these differing points of view result in the two different approaches to privacy. *Id.*

91. *See* Reidenberg, *supra* note 22, at 787 (suggesting inadequacies of the U.S. self-regulation approach); *see also* Shimanek, *supra* note 57, at 465-71 (noting that no comprehensive right to information privacy exists in the U.S.). In contrast to regulating *individuals*, Professor Fred Cate notes that the U.S. historically depends on "private industry, private property, and individual self-reliance." Cate, *supra* note 8, at 223. Cate further argues that "Constitutional rights are generally negative; they do not obligate the government to do anything, but rather to refrain from unnecessarily interfering with individuals' freedom to act." *Id.*; *see also* Samuelson, *supra* note 61, at 1127-1128 n.14. (stating that many Americans prefer the market-based approach). *See, e.g.*, Thomas Reith III, *Consumer Confidence: The Key to Successful E-commerce in the Global Marketplace*, 24 SUFFOLK TRANSNAT'L L. REV. 467, 477 (2001).

92. Shaffer, *supra* note 6, at 27.

93. *See* Cate, *supra* note 7, at 881 (noting that across-the-board rules and regulations are usually not sufficient, because they do not achieve their purpose and fail to provide sufficient solutions). Ultimately, the court must make an independent inquiry into the facts and circumstances of each case when constitutional rights are at stake. *Id.*

94. Cate, *supra* note 7, at 887 (stating that general distrust of the government results in a preference for market-based solutions); *see also* Rose, *supra* note 41, at 446 n.7 (arguing that the self-regulation approach remains superior in the digital age, because "private efforts of industry working in cooperation with consumer groups are preferable to government regulation"). (citations omitted). The right to privacy expands slowly, as Congress has rejected numerous attempts to enact omnibus regulation.

American values.[95] Couched in distrust of large government and the belief that the government should *first* show actual interest in regulating privacy, the U.S. system differs from that of the EU.

1. Distrust of Large Government[96]

The possibility of the government surreptitiously monitoring individual behavior or controlling personal information concerns many Americans.[97] The general distrust of a large and powerful government,[98] with unfettered discretion to monitor potential impositions on privacy, leads courts to scrutinize proposed privacy regulations carefully.[99] Relying more on market controls and self-regulation, a less-is-more approach to governmental control over private information underlies American privacy law.[100]

2. The Government Must Show Some Actual Interest in Regulating Privacy

Whether infringement arises from actual monitoring of behavior or via strict regulations or laws, courts generally require the government to show more than a modicum of interest in regulating privacy.[101] Instead, the government must demonstrate a compelling government interest to infringe these rights.[102] Hastily passing

---

95. *See* Cate, *supra* note 8, at 174 (noting that public interest zealots and industry leaders clash over how much influence the U.S. government should have over privacy).

96. This Note is intended to address "normal" situations. For example, in a post–September 11 world, many citizens welcome more government influence than they would ordinarily. Government initiatives, like the Patriot Act, the FBI's Carnivore technology, and the National Strategy to Protect Cyberspace all represent a possible shift (at least to some extent) of U.S. norms regarding government influence in personal privacy.

97. *See supra* notes 96-98 and accompanying text.

98. *See We Know You're Reading This: Privacy Issues*, ECONOMIST, Feb. 10, 1996 ("Trusting the government with your privacy is like having a Peeping Tom install your window blinds.") (citations omitted), *available at* 1996 WL 8670907. Other U.S. values conflict with the right to privacy. Even if these other valued did not exist, the principle of a limited government still stands in the way of creating a government privacy agent. Cate, *supra* note 8, at 226; *see* Samuelson, *supra* note 61, at 1173 (arguing that Americans' interests in information privacy conflict with the desire for a strong information economy).

99. *See, e.g.*, Shaffer, *supra* note 6 (noting that Americans distrust centralized government involvement in the data privacy arena); *see id.* at 23 n.82 (providing a discussion of why U.S. citizens distrust the government and why U.S. privacy laws remain market-based).

100. *See supra* note 92 and accompanying text.

101. *See infra* note 140 and accompanying text.

102. *See infra* note 136 and accompanying text.

legislation may prove harmful in the cyber age.[103] Many advocates seek a middle ground, as the risk of maintaining two competing privacy regimes creates a precarious situation.[104] With these considerations in mind, the FTC and the EU negotiated a common ground—the Safe Harbor, a voluntary method for U.S. companies to comply with the Directive—a solution which stands in stark contrast to strict, overarching, binding regulation sought by privacy advocates.

3. The Safe Harbor Solution

As the U.S. and the EU disagree on how to regulate Internet privacy, extensive negotiations between the two entities produced the Safe Harbor, which provides a voluntary alternative for U.S. companies that want to do business in Europe in spite of the dictates of the EU Directive.[105] Seven fundamental principles are embodied in the Safe Harbor. The specific provisions are: (1) notice, (2) choice, (3) onward transfer, (4) security, (5) data integrity, (6) access, and (7) enforcement.[106]

Three main concerns cause companies to hesitate joining the Safe Harbor: (1) the cost of joining, (2) the jurisdictional hook, and (3) the fact that, to date, only a small number of companies have certified. Safe Harbor presents another set of problems, however, for U.S. companies that certify themselves under its provisions. In order to comply, companies must incur substantial costs to ensure that their data management processes meet threshold requirements.[107] Companies view these entry and transaction costs as a major impediment to joining.

Further, certifying companies subject themselves to an entirely new set of regulations and a new jurisdiction, because they must still adhere to member state law if they maintain a physical presence

---

103. Protecting privacy requires that the government "proceed cautiously rather than run pell-mell toward new laws that risk unintended and self-defeating consequences." Winer, *supra* note 63.

104. Winer, *supra* note 70.

105. *See, e.g.*, Shah, *supra* note 28.

106. For a detailed description of each of these principles, see U.S. DEP'T OF COMMERCE, SAFE HARBOR, *at* http://www.export.gov/safeharbor/sh_overview.html (last visited Mar. 3, 2003).

107. Loomis, *supra* note 26, at 5. *See id.* (noting that Microsoft spent over one-half million dollars to comply witb the Safe Harbor). In addition, companies must incur substantial administration/disclosure costs to ensure ongoing compliance with the Safe Harbor. *Id.* Safe Harbor requires companies to post privacy policies that identify them as Safe Harbor companies, and they also must file a self-certification letter with the Department of Commerce. Bro, *supra* note 61, at 328.

there.[108] In addition, by certifying, companies consent to FTC jurisdiction.[109] Companies that participate view this broadened jurisdiction as a disincentive because they *involuntarily* subject themselves to higher scrutiny than under current U.S. law, while the FTC does not subject non–Safe Harbor companies to these additional constraints.[110] Finally, many companies see no upside to joining the Safe Harbor because an insignificant number of companies have certified to date.[111] In sum, certification under Safe Harbor does not create a long-term value proposition[112] for many companies. As the Directive and similar regulations like the Safe Harbor fail to garner industry support, EU-style regulations also face strict constitutional challenges—for example, under the First Amendment principle of free flow of information.

V. THE EU DIRECTIVE AND THE FIRST AMENDMENT

The EU Directive clashes directly with the First Amendment principle of free flow of information and vests power in the government rather than in the individual. Justice Brandeis defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and what extent information about them is communicated to others."[113] While this definition sufficed in a world that dealt only with actual physical contact or intrusion into people's homes, it fails to explain fully the privacy concerns in an on-line environment.[114] As the status of privacy law on the Internet remains in flux, many privacy advocates argue for a

108. *See* Judy & Hayes, *supra* note 35 (noting that a significant problem arises because companies who qualify themselves become subject to enforcement actions by other government entities). Further, while the Safe Harbor keeps companies from having to register with data protection authorities in the EU, those companies are still subject to any country's local law in which tbey have a physical presence.

109. *See supra* note 34 and accompanying text.

110. As a result, companies certified under the Safe Harbor not only must elevate their data protection to comply with EU law, but they also must institute this higher protection in the U.S., thereby subjecting themselves to a higher standard in the U.S. Judy & Hayes, *supra* note 35.

111. U.S. DEP'T OF COMMERCE, SAFE HARBOR LIST, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (providing a list of the 328 companies that have joined the Safe Harbor ranks) (last visited Apr. 15, 2003). Industry has embraced these principles in a lethargic and unentbusiastic manner, and its view can be summed up in the statement by a partner at the law firm of Proskauer, Rose: "It's not obvious that the benefits [of Safe Harbor] outweigh the costs." Loomis, *supra* note 26, at 5.

112. For a definition of "value proposition," see *supra* note 43 and accompanying text.

113. Cate, *supra* note 7, at 877 (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM (1967)).

114. *Id.* at 877; *see* Saleem, *supra* note 9, at 176 (noting that theories concerning the appropriate solution are in a state of flux).

broader, more omnibus legislative solution.[115] However, this approach conflicts with the bedrock First Amendment[116] policy concerning the free flow of information.[117]

Alhough it is not absolute, American citizens cherish this right to privacy[118] and are suspicious of government.[119] Adopting an all-encompassing privacy regulation would contravene these First Amendment rights.[120] As Solveig Singleton recognized, "[a]n omnibus system of privacy regulation would mark an extremely radical change in the legal framework for the flow of information through the economy."[121] Many privacy advocates, however, tend to downplay this principle when analyzing the EU Directive.

Citing consumer respect and consumer safety, many U.S. privacy advocates lobby for legislation tightening on-line privacy controls yet tend to ignore the current "free-flowing" infrastructure in which U.S. companies operate. These advocates also ignore the constitutional hurdles that limit the passage of broad legislation. The First Amendment certainly does not preclude all legislation or regulation in the privacy context, but it does pose a significant hurdle to overarching information privacy legislation, or regulation similar to the Directive.[122] Courts generally subject any type of regulation encroaching on First Amendment values to the highest level of scrutiny.[123] However, many consumers and privacy advocates believe that the sheer amount of information that companies collect about

---

115. *Cf.* Reidenberg, *supra* note 22, at 787 (arguing against the self-regulation model and advocating a solution that utilizes a combination of law and technology).

116. *See, e.g.*, Kirtley, *supra* note 52, at 644-46 (noting the general First Amendment preference for the free flow of information).

117. *See, e.g., supra* note 9, at 23 (describing how several business groups opposed a comprehensive privacy law because of First Amendment issues). Although legislation similar to the EU Directive was suggested in Washington, those bills were rejected and received heavy opposition from the Privacy-Plus Coalition. *See* Barbara S. Wellberry, *Bridging the Difference: The Safe Harbor and Information Privacy in the United States and the European Union*, PRIVACY & INFO. L. REP., Feb. 2001 (stating that the First Amendment requires a balance between individual privacy rights and the free flow of information).

118. Wellberry, *supra* note 117.

119. *See id.*

120. Singleton, *supra* note 15, at 133.

121. *Id.* at 133-34.

122. *See, e.g.*, Cate, *supra* note 8, at 203-204 (discussing the First Amendment implications of proposed broad legislation).

123. This scrutiny involves a detailed analysis into the facts of each case and requires careful judicial review. *See* Cate, *supra* note 7, at 880-81 and accompanying text; *cf.* Ronald Krotoszynski, Jr., *Identity, Privacy, and the New Information Scalpers: Recalibrating the Rules of the Road in the Age of the Infobahn: A Response to Fred H. Cate*, 33 IND. L. REV. 233, 240 (1999) ("[T]he First Amendment value in distributing highly personal information about average citizens is, at best, very low.").

individuals and the way in which they use this information is cause for alarm, and in turn, greater regulation.[124]

It therefore seems that support for change in on-line business practices is growing as privacy advocates contend that the U.S. also needs a comprehensive approach to the regulation of data privacy, rather than its current method of post hoc reactions to market demands.[125] As one scholar notes, "reliance on self-regulation is not an appropriate mechanism to achieve the protection of basic political rights. Self-regulation in the U.S. reduces privacy protection to an uncertain regime of notice and choice."[126] Indeed, companies and legislators face a legal issue unique to the Internet, because companies and the government can accumulate vast stores of personal information with minimal effort and cost.[127]

Given this capacity to collect information in a previously unimaginable way, jurisprudential guideposts in the U.S. and abroad are shifting to create scenarios in which companies must watch over their shoulders before they use personal information. As cyberlaw scholar Pamela Samuelson noted:

> Work must continue on evolving norms about *appropriate and inappropriate* uses of personal data, on persuading firms that the trust necessary for electronic commerce to flourish requires the interests of individuals in information privacy to be given appropriate deference, and on adapting the technological infrastructure of cyberspace so that information privacy becomes easier to achieve. The principal challenge of these multifaceted endeavors is not to recreate in cyberspace some preexisting zone of privacy from the physical world, but to articulate values inhering in information privacy that should constrain and structure social, economic, technological, and legal relations.[128]

---

124. *See We Know You're Reading This*, *supra* note 98, at 27 (noting that privacy concerns arise not just from companies and other people accessing your information, but also from the government). The article provides a hypothetical of a "hero" consumer and the fear of information collected about him:

> On a typical day, for example, our hero's driving route may be tracked by an intelligent traffic system. At work, his employer can legally listen in on his business conversations on the telephone, and tap into his computer, e-mail, or voice mail. At the shopping center, the ubiquitous closed-circuit camera may soon be smart enough to seek him out personally. His clothes shop is allowed to put peepholes in the fitting rooms; some have hidden microphones, too. The grocery stores information about him if he is a member of its buyers' club.

Id.

125. *See* Shaffer, *supra* note 6, at 64 (noting that privacy advocates believe that the U.S. needs "a comprehensive approach to privacy protection, not a fragmented, scandal-specific one").

126. Reidenberg, *supra* note 41, at 726.

127. *See, e.g.*, Rose, *supra* note 41 (noting the vast amount of information to which on-line businesses have access); *see also* Cate, *supra* note 8, at 178 (noting the various types of information collected from on-line users).

128. *See* Samuelson, *supra* note 61, at 1129-30 (emphasis added).

Fortunately, broad legislation, such as the EU Directive,[129] has not been passed in the U.S., but many American privacy advocates still push for such legislation.[130] Some advocates even argue for a reasonable limit on the "seemingly ceaseless forward march of modernity."[131]

A. How Much Government Involvement?

Even if the public acquiesces to a curtailment of the free flow of information, a threshold question concerning the role of the government in privacy regulation lingers as the subject of heated debate.[132] "The critical question is whether 'new wine can be poured successfully into an old bottle,' or whether new legal norms must be devised for the governance of the Networld."[133] On their face, these proposals for broad legislation appear benign and purportedly represent the best interests of Americans despite their curtailment of the free flow of information. Congress and agenices should not institute broad regulation, however, without an appreciation of the historical balance between the interests of government and the individual.[134] The value added from data collection regulation must be weighed against the value of free flow of information.[135]

---

129. Krotoszynski, Jr., *supra* note 123, at 236-38; *see also* Cate, *supra* note 8, at 179, n.31 (noting that Internet users believe that the government should pass laws to protect privacy and noting that privacy will be the issue of the future, much as the environmental movement affected the twentieth-century industrial society). *Id.* at n.32.

130. *See* Shaffer, *supra* note 22, at 4.

131. *See, e.g.*, Krotoszynski, Jr., *supra* note 123, at 139, 239 ("As one commentator has wryly observed, reliance on market mechanisms and self-regulation to protect privacy is tantamount to 'putting Count Dracula in charge of the blood bank.' ") Krotoszynski argues that this movement runs akin to the labor union movement, and he states that people need the government to secure privacy rights, much as labor unions ensured parity between workers and management during labor negotiations. *Id.*

132. *See, e.g.*, Cate, *supra* note 7, at 880-83 (noting the pivotal question of what role the government should have in resolving this debacle).

133. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1647 (2001). *See, e.g.*, Saleem, *supra* note 9, at 196 ("[I]f the U.S. establishes a Federal Data Protection Agency to regulate privacy, the international scope and impact of such an agency must be thoroughly considered.").

134. *See* Cate, *supra* note 7, at 878; Bauchner, *supra* note 18, at 707 ("At the heart of this issue is an attempted balance between individuals' privacy and the need to transmit data relating to individuals, particularly in the Information Age.").

135. The U.S. government has acknowledged the need to halance personal privacy in network environments with such principles as the First Amendment free flow of information. Bauchner, *supra* note 18, at 712 nn.154-55; *see also* Cate, *supra* note 8, at 220 (noting that the free flow of data/information embodies the "cornerstone of a democratic society and market economy").

This principle applies both when the U.S. government seeks to collect information and, in the situation of the EU Directive,when it seeks to interfere with the collection or dissemination of information by private parties.[136] Although the government might not be the entity collecting the information, the government still interferes with the free flow of information when it enacts broad legislation that curtails information collection.[137] Thus, because courts subject regulations affecting the free flow of information in the private sphere to heightened scrutiny,[138] courts should also require that the government show a strong interest in the enactment of broad legislation.[139] This argument for heightened scrutiny is not to say that proposed privacy regulation will never pass muster under constitutional standards, but it is indicative of the hurdle that privacy advocates must overcome to enact such legislation or regulation.[140]

B. Privacy Versus the Ability to Learn About Your Neighbor

If a regulation similar to the EU Directive were implemented in the U.S., the regulatory framework would face serious problems under the First Amendment when the issue is analyzed from another angle. The First Amendment also historically protects the ability to freely learn about other people in ordinary business interactions and

136. The Directive regulates and inhibits the free flow of information collected by both companies and government. This regulation is in stark contrast to tbe current U.S. legal infrastructure. In the U.S., legislature usually imposes Constitutional *limits* (if any) on the free flow of information against the government, not against individuals or companies. Thus, it follows that the Constitutional guarantee of free flow of information is invoked when the government attempts to thwart the private sector from collecting information for personal or business reasons vis-à-vis broad, overarching regulations and legislation. *See, e.g.*, Winer, *supra* note 63. The Directive allows EU citizens to retain rights over their personal information that effectively inhibit, and in some cases, stop the flow of information by giving "them the rights to see, copy, correct, erase, and limit sharing of their personal data." *Id.* at 65.

137. *See supra* note 136 and accompanying text.

138. *See* Cate, *supra* note 7, at 881 n.12 (citing cases in which tbe Court applied heightened scrutiny).

139. "Laws that put in place broad restrictions on the flow of information, rather than require sensitive balances to prevent specified harms, are constitutionally problematic." *Id.* at 881.

140. *See* id. at 882. ("Laws that restrict that free flow almost always conflict with this basic principle. That does not mean tbat such laws are never upheld, but merely that they face a considerable constitutional hurdle."); *see id.* at 887 (noting that the court typically allows the free flow of information absent a compelling government interest to restrict information). A substantial problem involves balancing legitimate corporate interests in gathering and disseminating market information with individuals' interests to keep information about them private and outside of the public eye. David E. Brown, Jr., *From the Editor: Privacy, Commerce and the First Amendment*, ELEC. BANKING L. & COM. REP., MAY 2001.

in day-to-day contacts.[141] Contrary to privacy advocates' claims, the *collection* of information actually helps one learn about her neighbor, which can prevent false information from being spread. However, when addressing the Directive, many privacy advocates appear to seek a virtual world of complete anonymity in on-line transactions—a world in which one cannot link personal information back to an individual.[142] This solution not only runs counter to protecting the free flow of information, but it can actually cause problems with individual accountability.[143]

To support this proposition, Judge Richard Posner notes that privacy can sometimes impose serious costs on society.[144] He acknowledges that, in many cases, misleading people with whom one conducts business creates a motive to conceal information.[145] Posner argues that private information, if revealed, actually serves to correct misapprehensions about individuals.[146] Indeed, too much privacy can facilitate the promulgation of false information and can impose substantial costs on society.[147] Furthermore, Posner questions the actual harm of "casual prying," which he posits does not necessarily create a substantial threat (within reasonable limits).[148] According to Posner, "[p]rying enables one to form a more accurate picture of a

---

141. Restricting information flow usually raises First Amendment concerns, because the First Amendment allows individuals to learn about each other during business and other day-to-day occurrences. *See, e.g.*, Singleton, *supra* note 15, at 152.

142. *See* Reith, *supra* note 91, at 749 (stating that the EU tries to foster consumer confidence by "increasing transparency of on-line transactions").

143. Absolute anonymity could prevent on-line accountability, while full accountability could prohibit anonymity. Complete autonomy over information flow could stop individuals from accessing general information that is beneficial to society. Branscomb, *supra* note 133, at 1645.

144.

> Much of the demand for privacy ... concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is ... to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit.

Cate, *supra* note 8, at 221-22 (citing Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399 (1978)).

145. *Id.* at 221.

146. *Id.* at 222.

147. Privacy can cause the dessimination of false information, and it interferes with business's ability to make informed decisions based on individualized information. This interference creates transaction costs because companies then have to determine the accuracy of the information they *do* have. *Id.* In addition, future losses can result because of the inaccurate and incomplete information. *Id.*

148. *Id.* (citing Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 395-96 (1978)); *see also id.* at 222 ("Information is the lifeblood that sustains political, social, and business decisions.") (quoting Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 987 (1983)).

friend or colleague, and the knowledge gained is useful in one's social or professional dealings with him."[149] Under this view, *too much* privacy can be detrimental to society. The Directive's ramifications actually include lower quality of information being transferred, because the Directive grants consumers a veto power over others' ability to learn about them.[150] Unfortunately, this veto power could cause adverse effects on the market.[151] In sum, regulation of information disclosure often creates positive effects, but major problems do exist when regulating the actual *collection* of information. Recent scholarship has noted that requiring companies to disclose *how* information is used would meet applicable constitutional standards but that other restrictions, such as data collection restrictions, may not square with sound First Amendment policy.[152]

The traditional U.S. theory posits that each industry knows the best regulatory framework to implement with regard to data privacy in that industry's respective field.[153] In contrast, EU policymakers are concerned that this will ultimately incentivize companies to inject their consumers' information into an unregulated market, which could lead to exploitation of the consumers' information.[154] An EU-style

---

149. *Id.* at 222 n.314; *see also* Singleton, *supra* note 15, at 152 (maintaining that the collection of more information about consumers alleviates many security problems).

150. Cate notes the decline in the quality of information on-line that results from tightened regulation:

> Europe's experience shows us that the total effect of such regulations is a reduction in the amount and quality of information that has flowed freely in the shared domain between companies and consumers, or the prevention of the growth of such libraries altogether. The consumer is given a unique veto power over another's ability to learn about him or her, a power that cannot be granted without diminishing the freedom of others. Because we do not own information about ourselves as a general rule, this veto power represents a drastic upheaval in the normal rules of human society. Like a sudden broadening of privacy torts, copyright law, or trademark law, most proposed regulation shrinks the public domain. This conflict is seen between the expansion of copyright law or trademark law and free speech, but privacy law does not have the constitutional sanction that intellectual property law does.

Id. at 120-21.

151. *See* Winer, *supra* note 70 (noting that unnecessary regulation distorts the developing electronic marketplace and raises overall price levels for consumers and that false information in the market almost always causes adverse effects on consumers).

152. Numerous laws regulate information flow, but many of those laws require disclosure and the further dissemination of information rather than the quashing of it. *See* Cate, *supra* note 7, at 882 & n.26 (providing securities laws, banking laws, and insurance laws, inter alia, as examples of law and regulations that favor the free flow of information). Further, many academics believe that disclosure regulations are constitutional but that other restrictions regarding collection might violate the First Amendment. *See* Brown, *supra* note 140.

154. *See* Rose, *supra* note 41, at 446-48 (discussing the industry's sectoral approach to privacy regulation, and why this method of private individuals working with consumer groups is preferred to broad government regulation)

154. Bensoussan, *supra* note 12, at 299.

regulation in the U.S would invade the private sphere by preventing individuals from learning about each other, because the thrust of such legislation would regulate business entities rather than curtailing government influence. In contrast, individuals should be free to learn about each other in the marketplace, because, as Posner notes, this knowledge encourages accountability and helps to prevent promulgation of false information.[155]

C. Regulation of the Private Sphere Versus Constraints on Government

While some concern exists regarding business encroachment on individual privacy, most Americans view the government as a greater threat[156] to individual liberty than other individuals or companies.[157] In addition, the Constitution does not explicitly grant individuals a right to privacy, but the Supreme Court has interpreted certain provisions of the Constitution to provide some protection from *government* encroachment on individual privacy.[158] As a result, many Americans prefer decentralized authority and remain apprehensive about regulation of the private sphere.[159] Even when countries pass statutes regulating privacy, this regulation typically restrains the government, not private actors.[160] Without a compelling governmental

---

156. Richard A. Posner, *The Right to Privacy*, 12 GA. L.REV. 393, 399 (1978) (noting the importance of encouraging accountahility).

156. *See* Cate, *supra* note 8, at 220 (noting that the government, not individuals, presents the largest threat to individual liberty, which explains why many constitutional rights protect against government action).

157. *See* Cate, *supra* note 7, at 884-86 (noting that the Constitution typically monitors state action, not the individual sphere):

> One dominant theme of constitutional rights is the protection of citizens from government intrusion into their privacy. A vigorous First Amendment, for example, permits individuals the privacy of their own thoughts, beliefs, and associations. The Third Amendment keeps government soldiers from being quartered in private homes. The Fourth Amendment prohibits unreasonable searches and seizures. The Fifth Amendment restricts government from interfering with private property, provides for due process and compensation when it does so, and protects citizens from self-incrimination. Collectively, these and other provisions of the Constitution impose extraordinary limits on government authority to intrude on private property, compel testimony, or interfere with practices closely related to individual beliefs, such as protest, marriage, family planning, or worship.

Id. at 884-85.

158. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 52 (1997); *see also id.* at 49-66 (providing a detailed discussion of the constitutional limits on government encroachment into the private sphere).

159. *See* Wellberry, *supra* note 117 (noting that the U.S. adopts a decentralized wait-and-see approach and that individuals in the U.S. usually worry about excess government power and intrusion into privacy rather than excess power vested in private individuals).

160. *See, e.g.*, Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 26 (discussing the Privacy Act of 1974 and

interest, courts typically prefer the free flow of information over such broad regulation.

D. Can More Government Control Really Be the Answer?

The guiding principle of U.S. privacy norms lies in a less-is-more approach to government regulation of personal information.[161] Americans rarely favor broad legislation, and view governmental control over personal information as contrary to American values.[162] In contrast, the Directive requires each member state to create a national supervisory authority, known as a data authority,[163] to control personal data that companies seek to process.[164] The Directive requires companies to secure documented consent from individuals and present this information to the data authority before they can use the collected information.[165] In practice, the government authority (data authority) retains the information in its databases, and the individual actually *loses* control of her information to the government.[166] This loss of control effectively gives the government control over personal information, which contravenes traditional U.S. privacy norms and policies, thus creating further tension between the Directive and the traditional U.S. approach.

The EU's creation of data authorities actually gives the government more power over individuals' information.[167] Under the

---

noting that at that time, the country worried about "Big Brother," because the government wanted to compile a database which would serve as a centralized repository of records of U.S. citizens). As a result, Congress held hearings culminating in the enactment of the 1974 Privacy Act, which applied to the *government* and its collection practices. *Id.* It limited the extent to which the *government* could intrude into the private lives of its citizens. *Id.* The 1974 Act was a landmark accord for privacy legislation, but its breadth was limited to constraining the government as it set limits for collection, use, dissemination of personal information held or collected by government agencies. *Id.*

161. *See supra* note 93 and accompanying text.

162. *See infra* note 169 and accompanying text.

163. *See infra* notes 168-169 and accompanying text. The data authority acts as a surrogate of the government. Julia Gladstone, *The Impact of E-Commerce on the Laws of Nations Article: The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy*, 7 WILLAMETTE J. INT'L L. & DISP. RESOL. 10, 22 (2000).

164. *See infra* notes 169-170 and accompanying text.

165. *See supra* notes 81-82 and accompanying text.

166. *See infra* note 169 and accompanying text. The practical result is counterintuitive—while advocates want to protect privacy, they basically lose the right to any anonymity—if each company or person must get affirmative consent from each individual, this "consent" must be secured and verified somewhere and stored in a repository for documentation. *See* Johnson, *supra* note 10, at 22. This creates tension, because the information actually remains stored with the government. *Id.*

167. In theory, every business must get affirmative consent from each individual prior to collecting personally identifiable information from her. The company then must verify this

infrastructure established by the EU Directive, the government, through the data authorities, stores personal data.[168] Under this system, the data authority therefore acts as a surrogate for the EU, because the Directive requires that each member state create an independent public authority that supervises data flows, retains investigative power over data processing, and retains the ability to access the data.[169] The system aims to create uniformity, but the Directive in fact grants the government the power to store the information. This transfer of power would create a problematic situation in the U.S., because the EU method of registering data processing activities does not align with American values of minimal government intrusion into the private sphere.[170] Because the Directive requires that companies or persons who wish to "collect, process, use, store, and disseminate personal information" register with a government entity, the Directive contravenes the U.S. constitutional framework.[171]

Member states' differing laws only exacerbate the problem.[172] EU countries remain free to establish varying levels of privacy. For example, Italy's provisions are stricter than those provided in the Directive.[173] Italian laws state that individuals must give consent in writing, but "such processing must be specially authorized by the

---

consent with its local data authority. This information/documentation of consent must be stored in databases *somewhere*, since it is stored with the data authority, a public authority, the individual loses her right to anonymity on-line. *Id.*

168. *See infra* note 169 and accompanying text.

169. Cate describes the contours of the EU framework:

> Each member state must establish an independent public authority to supervise the protection of personal data. Each 'supervisory authority' must have, at minimum, the power to investigate data processing activities, including a right of access to the underlying data, as well as the power to intervene to order the erasure of data and the cessation of processing, and to block the proposed transfer of data to third parties.

Cate, *supra* note 8, at 183. Ultimately, this gives a substantial amount of power to a delegated authority of the government. *See id.* at 183-84 nn.56-57.

170. *See* Rose, *supra* note 41, at 469-70 (noting that self-regulation intrudes less into individuals' lives than mandating that companies that collect information notify the government).

171. *See* Cate, *supra* note 8, at 226 (noting that the EU scheme is antithetical to the U.S. constitutional scheme for privacy, because the freedom of expression and freedom from government intervention trumps the government's right to intrude into individuals' lives).

172. *See* Cate, *supra* note 8, at 195. *But see id.* (noting that although the U.K. law is much more detailed, it really does not affect what level of privacy is afforded—it does, however, leave less to a national authority with regard to discretion on data collection); *id.* at 230 (arguing that direct government oversight does not provide proper privacy protection). These different laws are discussed more fully in Part VI.

173. *Id.* at 194-95.

national government's supervisory authority."[174] This scenario results in uncertainty in the law—even more so when different member states enact varying levels of protection.[175] In sum, many privacy advocates push for broad legislation under the guise of civil liberties without acknowledging a long-standing U.S. maxim: Strong distrust of a centralized government with unfettered discretion over personal privacy counsels against vesting greater authority to regulate on-line privacy in a centralized government body.[176] Implementing an EU-style regulation in the U.S. poses a difficult challenge under First Amendment principles.[177] In addition to these problems, a closer look at the Directive and the infrastructure that it supports reveals that the Directive fails to achieve its articulated goal of uniformity in the regulatory framework.[178]

VI. THE EU DIRECTIVE AND THE STATED GOAL OF UNIFORMITY

The Directive does not achieve the goal of uniformity for two reasons. First, the standards[179] vary among member states. Second, deference to the interpretations of multiple, member state–specific data authorities erodes uniformity. These two issues work in tandem to cause the Directive to fail in its stated goal of uniformity in the regulatory frameworks of EU member states. A similar system here in the U.S. would also likely fail in the same regard.

---

174. *Id.*; *see also* Reidenberg, *supra* note 41, at 736 (noting that the Directive gives national supervisory authorities (independent agencies) significant interpretive power).

175. *See* Bloss, *supra* note 42, at 650-51 (contending that EU citizens trust administrative bodies more than Americans trust them).

176. Cate, *supra* note 8, at 226, n.330 (quoting Jane E. Kirtley, *The EU Data Protection and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648-49 (1993)).

> Privacy advocates urge the adoption of the European model for data protection in the name of protecting civil liberties. But in so doing, they ignore, or repudiate, an important aspect of the American democratic tradition: distrust of powerful central government . . . . [W]hen it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart . . . . The European paradigm assumes a much higher comfort level with a far more authoritarian government.

Id.

177. *Id.* at 226 (noting that persons who collect information must then register the data with a national supervisory authority, and so control is placed with the government, not the individual).

178. Generally, uniformity aids in providing predictability, ease of enforcement, and congruity in the law.

179. In particular, the "adequacy" standard can vary significantly between member states. Shimanek, *supra* note 57, at 464-65.

The Directive seeks to provide uniformity in data practices throughout the EU.[180] This goal is similar to the U.S. federal system, in which there exists an overarching goal to create and maintain predictability and uniformity among various state bodies of law. Uniformity allows individuals and companies to rely on existing laws and not be concerned with varying standards in different states or countries. However, the Directive fails to provide uniformity along these lines.

Implementation of an EU-style regulation in the U.S. is unlikely to fulfill the desire for uniformity: much like the emperor's weavers touted their magical cloth, the EU praises the Directive's "uniformity," even though the Directive is not uniform. Many U.S. privacy advocates "see" this new set of clothes, so to speak, but refuse to acknowledge its shortcomings, such as the lack of uniformity. The fundamental problem lies in the fact that the Directive allows for individual member states to enact their own privacy laws, so long as these laws do not provide less than Directive's threshold protections.[181] Under the Directive, member states provide the actual substantive law for data transfer, not the EU.[182] On its face, this requirement does not appear to pose an insurmountable problem, but a closer analysis reveals the Directive's failure to provide for any real uniformity.[183] Because each member state applies its own substantive law, different member states create varying data protection levels.

This variation creates a dilemma, because the system results in agencies that operate independent of one another, which gives power back to the government by giving these authorities a "degree of interpretive power over any individual case."[184] Since the Directive affords them this broad interpretive power, it follows that their own legal traditions will taint their adjudications. This discretion allows agencies to inject member state law as well as national norms and

180. Bauchner, *supra* note 18, at 690 (noting the articulated goal of uniformity).

181. *See* Shimanek, *supra* note 57, at 464-65 (noting that a single member state can choose to implement stricter policies than the EU Directive itself, which creates a situation in which a single member state can effectively trump or veto other countries' laws); *see* Gladstone, *supra* note 163, at 18 (discussing the lack of uniformity in the EU, because each member state must pass its own legislation).

182. *See* Gladstone, *supra* note 163, at 18.

183. *See* Bauchner, *supra* note 18, at 690, 704-05 (noting that the articulated goal of uniformity is not the likely outcome).

184. Reidenberg, *supra* note 41, at 736 ("While a European level decision is supposed to apply in each Member State, the national supervisory authorities are independent agencies and will still have a degree of interpretive power over any individual case.").

interpretations into the mix rather than interpreting the Directive itself.[185]

For example, France and Germany require higher and stricter levels than Italy requires.[186] The Directive provides that no country may enact laws lower than the EU threshold, but it allows member states, at their discretion, to enact laws much stricter than the underlying EU rule of "adequacy."[187] This flexibility causes the EU to fall short of its intended goal of uniformity; indeed, the local laws of the member states display everything *but* uniformity—thus dismantling the façade that the Directive creates.[188]

As a result of this variation, companies operating in more than one EU member state must follow the strictest country's law, not the EU's law.[189] This instability defeats the purpose of a "uniform" system.[190] As the level of uniformity decreases, so does the law's predictability. While many argue that the Directive's uniformity is its

185. Angela R. Broughton et al., *International Employment*, 33 INT'L LAW. 291, 296 (1998); Cate, *supra* note 8, at 192-96 (providing an excellent discussion of various member states' laws, ranging from Italy to Sweden to Portugal and discussing nuances in the laws implemented by these countries).

186. *See* Shaffer, *supra* note 7, at 5 n.10 (noting that France and Germany also demand a higher threshold than other countries such as Italy). For case studies regarding the differing privacy practices in these respective countries, see *id.*; *see also infra* note 188 and accompanying text.

187. *See* Directive, *supra* note 1, at 25(1) (noting that each member state must provide adequate protection). However, tbe Directive provides littIe guidance as to what constitutes adequate. The final arbiter interprets subjective terms such as adequate. A major problem exists not only with ascertaining the meaning of adequate, but also witb the fact that member states may adopt stricter standards should they choose to do so. *See* Winer, *supra* note 63 (acknowledging the problem of differing standards). Further, different privacy standards often end up in the dustbin because they are either unenforceable or ignored. Thus, these standards can actually destroy privacy because they are neither consistent nor predictable. *Id.*; *see also* Bauchner, *supra* note 18, at 704 n.100 (stating that states are given the right to implement even stricter rules if they wish); James A. Harvey & Kimberly A. Verska, *U.S. Firms Weigh Their Options on EU Data Privacy Obligations*, COMPUTER & INTERNET LAW., Apr. 2001, at 17 (stating that countries such as Spain and Portugal enact very strict regulations and impose heavy fines, wbile other countries utilize less strict guidelines). *See generally* Directive Article 5.

188. *See* Johnson, *supra* note 10, at 21-22 (comparing Sweden's laws with other member states' laws).

189. The country that decides that it wants the strictest rules for data privacy wins, while the U.S. (or any other "third" country) must comply with her rules/regulations in order to do business in that country. Ultimately, it erodes the concept of uniformity that U.S. privacy advocates have come to cherish—as well as one of the fundamental tenets of the Directive.

190. *See infra* notes 199, 202 and accompanying text. Lack of uniformity invites lax enforcement and leads to endless litigation. Lack of enforcement then naturally leads to complacence in the implementation of the principles. The principle of uniformity thus defeats itself. However, one argument is that this system really creates uniformity to the strictest principles, rather than eroding uniformity. This argument lacks persuasive value, bowever, as it creates a slippery slope such that no, or very little, information can be transferred if countries can trump each other repeatedly when enacting laws to comply with the Directive.

greatest virtue, it may, in fact, be its weakest element. One scholar even noted, "[t]his is a far cry from the uniform data protection standards anticipated by the Directive's proponents."[191]

The EU Directive inevitably facilitates nonuniformity by virtue of its infrastructure as described above. This nonuniformity results because, as a practical matter, if a business wants to engage in on-line trade within any EU member state, the business must comply with that member state's data privacy rules, regardless of whether that state imposes stricter rules than other member states or than the Directive itself.[192] Under this system, one member state can effectively trump the laws of the other member states and consequently force other member states to raise data standards to the strictest level.[193] Delegating to member states a quasi-veto power over the laws of another member state creates friction between the member states because any member state could hypothetically raise the bar to an arbitrary level.[194] Thus, the degree of data protection a country is able to invoke is limitless.[195] In the event that other member states do not raise the bar to this level, nonuniformity results, and the stated purpose of the Directive is undermined.[196]

Sweden serves as an example of a country that fosters such nonuniformity. Swedish national law makes it illegal to mention information about any identifiable individual on the Internet without prior permission.[197] Clearly, this is a stricter standard than other member states impose. The application of this law led to inconsistent

---

191. Cate, *supra* note 8, at 195.

192. *See* Shimanek, *supra* note 57, at 465 n.79 (noting that each member state decides on its own what is considered adequate, that the result ultimately turns on how strict the member states, as individual entities, decide they want their laws and regulations to be, and that the functional effect is that a single member state can have a veto power); *see id.* at 465 (noting that if one member state actually enforces their laws strictly, the U.S. could suffer a huge setback). Another example of nonuniformity hides in the nomenclature itself: data collected from "identifiable persons" is subject to the Directive's hand, yet the term "identifiable person" is not uniform across the member states. Reidenberg, *supra* note 22, at 785; *see id.* at 785 n.67 (noting that the Directive does not solve all of the ambiguity and divergence).

193. Bauchner, *supra* note 18, at 704-05 n.104 ("Since each Member State is responsible for determining a third country's adequacy, such unavoidable 'disparities' in regulations among Member States means the adequacy requirement could be raised to meet the highest bar established by any single Member State."); *see supra* note 192 and accompanying text.

194. *See supra* notes 192-193; *see infra* note 196 and accompanying text.

195. Bauchner, *supra* note 18, at 705.

196. *See, e.g.*, Judy & Hayes, *supra* note 35 (noting that a significant problem is that some member states use the Directive as a *model* for their own laws, instead of following the Directive strictly and that some member states do not even have their own privacy laws).

197. *See* Johnson, *supra* note 10, at 22 (noting that Sweden was implementing the Directive via their own national law).

results across the EU.[198] When the Swedish government arrested fur protesters, after they advertised a boycott of certain fur producers and identified those fur producers by name, conflict resulted. This variance occurred because identifying fur protesters by name is not problematic in other member states.[199] While it is debatable whether mentioning fur producers by name raises any real privacy concerns, the practical result is that, under the Directive, other countries must conform their data practices with Sweden's regulatory framework. This requirement either will create a situation of maximum privacy or it will erode uniformity, but neither outcome represents an optimal solution. With respect to this particular issue, Sweden holds the proverbial "queen of hearts" in that it can effectively force, or at least exert substantial pressure upon the other member states, to increase the level of regulation. The EU institutes these policies at the risk of arbitrary lawmaking, which destroys rather than facilitates uniformity, because "small divergences and ambiguities will inevitably exist where the principles must be interpreted by different supervisory agencies in each of the member states. These remaining divergences in standards can pose significant obstacles for the complex information processing arrangements that are typical in electronic commerce."[200] Even the EU officials have even stated that the Directive is "ill suited to a far flung, inherently global medium such as the Internet."[201]

According to this analysis, the Directive creates a recipe for arbitrariness and may erode the stated goal of uniformity in on-line privacy regulations among EU member states. Again, the practical effect of this procedural framework is the erosion of uniformity.[202]

---

198. *See id.*

199. *Id.* Certain member states maintain national law at a macrolevel *and* national laws that deal with specialized topics in privacy (and other countries do not) which exacerbates the problem. Christopher Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 INT'L LAW. 79, 81 n.10 (2001) (advancing the proposition that the Directive ultimately lacks uniformity and providing a discussion of countries like Germany which have special laws for certain topics such as the Teleservices Data Protection Act, which can be found (in German) at www.eed.de.iukdg/gesetz/iukdg.html). Member states also write recommendations and pronouncements, which are like dicta in Supreme Court opinions, because while they are not law, they are persuasive in practice. *Id.* at 81 n.10-11. Not all of the member states have laws that are this strict on a particular or specialized topic of privacy law.

200. Reidenberg, *supra* note 41, at 734 (noting the difference in scope of the term "identifiable person" distorts companies' ability to process information).

201. Cate, *supra* note 8, at 230.

202. *See* Broughton et al., *supra* note 185, at 297.

> [F]rom the point of view of individuals and private employer companies, the directive has no teeth until a member state implements it. And the member states have latitude to implement the directive in varying ways—so that ultimately, for example, France's data privacy law (and the bureaucracy set up under it) will likely look significantly different from, say, Germany's.

Even if lawmakers overcome this problem and achieve uniformity, serious implications still exist if member states do not enforce their regulations or enforce them to differing degrees. As a result, U.S. companies likely will not adopt the Directive's principles, unless all of the member states adopt them as well.[203]

VII. THE EU DIRECTIVE LACKS ADEQUATE ENFORCEMENT MECHANISMS

While creating stringent regulations for data collection and dissemination, the Directive lacks a coherent enforcement structure.[204] Without effective enforcement mechanisms, the substantive law of online privacy regulation lacks practical applicability and fails to protect the public in any meaningful way. Without enforcement mechanisms, the law also provides little incentive for companies to adhere to its dictates.[205] While the EU created broad regulations and legislation, it does not enforce its provisions in the way that privacy advocates are led to believe.[206] In some cases, member states either do not enforce their national laws or enforce them to varying degrees.[207] In certain instances, member states do not enforce their national laws for business reasons; in other situations, the member states do not yet have an infrastructure to enforce the Directive or even have existing national law. [208]

Id.

203. *See* Harvey & Verska, *supra* note 187, at 18.

204. *See* O'Brien, *supra* note 4, at 89 (noting that complete nondisclosure of information is never necessary, not desirable, and virtually impossible to enforce).

205. *See* Harvey & Verska, *supra* note 187, at 18-19. Several EU states do not maintain substantial and extensive privacy policies and even where there is legislation, little enforcement exists. *See id.* at 19. Some countries, such as Spain and Portugal, invoke strict regulations and impose heavy fines, while other countries like the UK and France impose very few sanctions. *See id.* Winer offers a cynical view: "Or, as they say on Mars, where the EU has talked the talk, the U.S. has walked the walk. Lawyers who practice commercial law involving international business see this every day." Winer, *supra* note 76.

206. *See, e.g.*, Loomis, *supra* note 26, at 5 (pointing out that critics argue that member states do not comply fully with the registration obligations).

207. *See infra* note 213; *see also* Harvey & Verska, *supra* note 187, at 18 (noting a lack of compliance in the EU itself—few EU websites provide the required notices regarding disclosure and use of personal data). A dearth of hard evidence exists from EU reports or industry reports that a vast number of European companies are rushing to ensure wide-scale compliance projects. Until the EU companies start to adopt their own principles in their entirety, it is unlikely that U.S. companies likely will move up to a higher threshold of data privacy. *See id.* Several EU states have not adopted legislation, and even where legislation exists, little enforcement occurs. *Id.* For example, the U.K. and France received numerous complaints about data abuse, but few result in sanctions or even investigations. *Id.* at 19.

208. *See supra* notes 201-203 and accompanying text.

This lack of enforcement begs the questionof why U.S. privacy advocates encourage the adoption of similar provisions.[209] Moreover, U.S. companies view the lack of enforcement in Europe as a disincentive to conform to the EU Directive. As one scholar has noted, "[t]he lack of resources for government enforcement, especially when confronted with such widespread data processing, further diminishes the likely role of the [D]irective as an effective means of protecting privacy on-line."[210] This lack of enforcement in the EU makes the Directive an ineffective solution to privacy concerns in the EU, and, more importantly, in the U.S.[211]

This deficient enforcement mechanism weakens the ability of the European Union to regulate companies outside of Europe, because "[u]ntil it gets its own house in order, the EU would have a tough time trying to enforce the Directive against companies overseas."[212] Further, while more of the member states enact legislation in compliance with the Directive, neither the level of implementation nor the enforcement[213] is completely effective. As a result, U.S. companies halted their sudden rush to comply with the Directive, because they became aware of the significant enforcement problems in the EU.[214]

Many possible reasons exist to explain the Directive's lack of enforcement. One possibility is that in the EU, "there are disincentives to litigation. If a plaintiff files and loses, the plaintiff generally pays the costs for both sides."[215] This actually creates a disincentive for private individuals to bring claims. However,

---

209. *See infra* note 209 and accompanying text.

210. Cate, *supra* note 8, at 230-31.

211. If countries in the EU that adhere to the Directive do not enforce their own regulations either because they lack the infrastructure or because they simply choose not to enforce it, little incentive exists for a U.S. (or a third country) business to achieve a higher threshold of data protection. *See* Kuner, *supra* note 199, at 82-83 (noting that national or local authorities at the member state level lack resources and personnel to engage in widespread enforcement and that it is also difficult to monitor compliance because of Internet traffic).

212. Loomis, *supra* note 26, at 5 (quoting John T. Bentivoglio, of counsel at the law firm of Arnold & Porter, discussing the EU Internet privacy Directive).

213. *See* Reidenberg, *supra* note 41, at 734-35. As Internet law scholar Joel Reidenberg noted,

> Compliance with the national laws has also been an issue in Europe. The notice and registration requirements, in particular, appear to have a spotty reception. One study conducted for the European Commission questioned whether data processors were adequately notifying their treatment of personal information to the national supervisory authorities, and a recent study by Consumers International found that European Web sites were not routinely informing web users of their use of personal information.

Id.

214. Loomis, *supra* note 26, at 5 (acknowledging that the lack of enforcement removes any sense of urgency for U.S. firms to comply).

215. Winer, *supra* note 70.

regardless of the reasons, the EU does not effectively enforce the Directive.[216]

VIII. CONCLUSION

The EU Directive represents an on-line privacy system that clashes directly with the U.S. data privacy infrastructure. Like the public who could clearly see the emperor's nakedness but who pretended not to, many U.S. privacy advocates push for a similar system in this country. A piece of legislation similar to the Directive will not work in the U.S. because of the potential First Amendment violations. Simply put, legislation similar to the Directive contradicts traditional American privacy values and interferes with the touchstone of First Amendment principles—the free flow of information. Further, the Directive does not achieve its articulated goals of uniformity and the protection of fundamental rights. Instead, its procedural framework erodes uniformity.

The Directive's weavers, while claiming that they possess a cure-all for privacy concerns, advocate the implementation of a similar system in the U.S. The Directive, however, is a façade—an unfortunate truth that privacy advocates refuse to recognize. The emperor paraded through the town wearing nothing, yet the crowd looked beyond the emperor's folly and praised his "new clothes." Likewise, privacy advocates appear naked without *their* clothes, because they adamantly encourage identical legislation in the U.S. that cannot function.

---

216. Interview with Steven Hetcher, Associate Professor of Law, Vanderbilt University Law School, in Nashville, Tennessee (Dec. 23, 2002). A substantial real-world difference between the U.S. and the EU is that a similar legislative action in the U.S. would invite massive amounts of class action litigation. *Id.* Currently, in the EU, the Directive has not produced such a result. *Id.* However, for U.S. companies, this risk of class action litigation remains, arguably, the biggest fear of all. *Id.* If Congress passes a broad piece of legislation, every individual could, and likely would, sue. *Id.* Legislation like the Directive would therefore obviously cause catastrophic problems in the U.S. *Id.*

The children, however, unmoved by public sentiment, recognized the truth and spoke their mind. Likewise, opponents recognize the shortcomings of broad, EU-style privacy legislation and therefore seek to tear down the façade for the sake of finding a real, workable privacy solution.

David Raj Nijhawan[*]

* J.D. Candidate, Vanderbilt University Law School, 2003. Special thanks to God, my parents, Pradeep and Bev Nijhawan, my sister, Sunita Renee Nijhawan, my brother-in-law, Christopher Blanford, my grandparents, Bal Raj and Pushpa Nijhawan, my aunt and uncle, Pramodh and Nancy Nijhawan, John Raj Nijhawan, Phoebe, the Honorable Randy J. Holland, the Vanderbilt Law Review, Elizabeth TeSelle, Professor Steven Hetcher (for the title and the idea), Professor Patrick Duparcq (for encouraging me to consider law school), Mary Miles Prince (for teaching me how to Bluebook), Brenda Phillips, Thomas Francis Lomhardi (for his red pen), Thomas Wedeles (for his time spent editing this Note), James Frank Cirincione (for providing valuable comments throughout this process), Jeffrey Bush, Evan Bennett, Debbie Reule and Russ Miller (for editing earlier drafts), Stephen Larson (for bouncing ideas back and forth regarding the intersection of law and technology), Laura Domm, Kirsten DeBarba, Jean Blackerby, Trish Luna, Michelle Lyons (my moot court partner, for teaching me how to write—again), Meg Pattison, Eric and Carrie Eisnaugle, Linda Lam, Jason Cincilla (for defending our country as a member of the U.S. Special Forces), J.D. Blair (for praying for me during law school), Lisa Bamford (also for praying for me to survive Law Review), James Andrew Beard (for teaching me how to walk), Heather Siukola, Allison Overdeck, Patrick Flanagan, Rich Padgett (for teaching me to believe in myself and to pursue this goal), Elizabeth Karavitis, Beverley Pugh, Sue Deason (for teaching me the value of hard work), Louise Freeman, Bruce Parkinson, Mike Parker, Joseph Fonte, Christopher Thomas (for the inspiration), Stuart Meyer of Fenwick and West LLP, Lou Holtz (for the 1988 championship season), Tyrone Willingham, Arthur Guinness, Neil Peart (for inspiring me to always strive to do my best, even if I burn my wings a little), and finally, Bono.