Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 15 *Volume XV*
Number 4 *Volume XV Book 4*

Article 5

2005

Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators

Flora J. Garcia

COMMENT

Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators

by Flora J. Garcia*

* Fordham University School of Law, J.D. expected May 2007. M.A., Journalism and Mass Communications, The University of North Carolina at Chapel Hill, 1996; B.S., Computer Science and Economics, Duke University, 1987.

INTRODUCTION

The different approaches to privacy in the United States and the European Union are deeply rooted in traditions much broader than the concept of privacy, such as the role of government in private life, the role of the press, and the freedoms that are afforded to the media generally.[1] This Comment explores those different approaches, utilizing the facts of *Case C-101/01 Criminal Proceedings against Bodil Lindqvist*,[2] a Swedish case sent to the European Court of Justice ("ECJ") that should serve as a warning to legislators in the United States concerned with protecting privacy. In *Lindqvist*, the scope, definition, meaning, and

[1] *Cf.* Arnulf S. Gubitz, *The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?*, 39 NEW ENG. L. REV. 431, 446–47 (2005) (discussing the United States' broad view of privacy as compared to the European Union's restrictive view).

[2] Judgment of the Court of 6 November 2003 in Case C-101/01 (Reference for a preliminary ruling from the Göta hovrätt): Bodil Lindqvist, OJ 2004 C7/3 [hereinafter *Lindqvist Judgment*].

application of the European Union's Data Protection Directive ("Data Protection Directive," "Directive," "Directive 95/46")[3] was tested for the first time.[4] The Data Protection Directive affects United States companies involved in data transfer[5] in the European Union.[6] The U.S. Department of Commerce has established Safe Harbor provisions to help companies discern the requirements for protection of European Union residents' data in non-E.U. countries.[7]

Part I of this Comment provides a history of the Data Protection Directive and associated European Union regulation regarding data privacy. Part I also discusses the definitions in the Data Protection Directive and the issues of third country transfer and "adequate" protection. Part I concludes with a discussion of the United States' Safe Harbor guidelines, which address the Directive's third country elements for companies that participate.

Part II explains the European Court of Justice's decision in *Lindqvist*, the case of a Swedish woman who was accused and found guilty of violating the Data Protection Directive. This Part will illustrate the interplay between the European Court of Justice's decision, the text of the Data Protection Directive and the

---

[3] Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

[4] JuNelle Harris, *Beyond Fair Use: Expanding Copyright Misuse to Protect Digital Free Speech*, 13 TEX. INTELL. PROP. L.J. 83, 120 n.235 (2004) ("*Lindqvist* . . . was the first case interpreting a national enactment of the European Union's Data Protection Directive.").

[5] "Data transfer" is not defined within the text of the European Union's Data Protection Directive. *See* discussion *infra* Part II.A.5. However, throughout the body of the Directive, transfer is used in discussions regarding the moving of information from one location to another. *See, e.g.*, Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1317, 1336 (2000). Processing, storing, collecting, and accessing all seem to be activities related to data transfer. *Id.* at 1336.

[6] *See*, *e.g.*, Marsha Cope Huie, Stephen F. Laribee, and Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 396. *See also* Data Protection Directive, *supra* note 3, at Chapter IV.

[7] *See* U.S. Dep't of Commerce, *Safe Harbor Overview*, *available at* http://www.export.gov/safeharbor/sh_overview.html (last visited May 5, 2005) [hereinafter Safe Harbor Overview]; U.S. Dep't of Commerce, *Safe Harbor Documents*, http://www.export.gov/safeharbor/sh_documents.html (last visited May 5, 2005).

comments filed with the Court regarding the *Lindqvist* controversy. Further, Part II addresses the limited guidance that multinational corporations and others concerned with data transfer in the European Union can take away from the decision and its commentary regarding the definition of "processing" and "transfer"; what activities might fall under exceptions of the Directive; and what the Court considers information regarding health.

Part III analyzes the European Court of Justice's reading of the Data Protection Directive in the *Lindqvist* case, showing that the Court offered less delineation and clarity than observers hoped. It argues that true privacy protection is not ensured by penalizing private citizens such as Lindqvist, but rather by increased awareness on the part of consumers and companies of both the massive quantities of data stored and the transfer of that data. Part III concludes that the *Lindqvist* decision should be treated as a warning to eager politicians in the United States who see an overarching law as the solution to privacy concerns.

I. EUROPE AND THE UNITED STATES: PRIVACY TRADITIONS ROOTED IN DISTINCT HISTORIES

The United States relies on homegrown features such as "the press, plaintiffs' bar and watchdog groups"[8] for protection of data privacy, a scheme that highlights United States citizens' "continuing . . . ambivalence about state power."[9] The contrasting European view of privacy as a human right—and hence of "data protection as a fundamental human right"—aids in understanding both the Data Protection Directive and attitudes in the European Union towards transgressions that violate the privacy of individuals.[10] In response to the Data Protection Directive, the United States Department of Commerce negotiated the U.S.-EU

[8] GLOBAL PRIVACY AND SECURITY LAW: SPECIAL REPORT PREPARED FOR THE 97TH ANNUAL MEETING AND CONFERENCE OF THE AMERICAN ASSOCIATION OF LAW LIBRARIANS S5 (BNA 2004).

[9] PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 211 (1996).

[10] *See* CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 16 (2003).

Safe Harbor Data Privacy Accord, which sets standards for companies wishing to transfer data out of Europe.[11] Companies that undergo Safe Harbor certification are considered under the agreement to have "adequate" safeguards in place.[12] Unlike the U.S. approach, national laws addressing privacy were passed in European countries by the early 1990s,[13] with some dating back to the 1970s.[14] These regulations generally were broad in nature, required registration with governmental offices, and were applied regardless of the data type.[15]

A. The European Union

Though much attention has been focused recently on the differences in privacy protection approaches and regulation with the advent of the Internet in Europe, concerns over other countries' inadequate treatment of personal information predate the ubiquity of the Internet.[16] Norway, Austria, Germany, Sweden, France and the United Kingdom all had blocked or prohibited data flows to at least one other country by 1990.[17] In Germany, the state of Hessen passed the first data protection law in 1970 amid fears of a return of the misuses of personal data that took place when the Nazis used early data sorting devices to establish Jewish ancestry.[18] Concerns about German history repeating itself led to the formation of governmental privacy protection agencies in all the states. By

---

[11] U.S. Dep't of Commerce, *Welcome to the Safe Harbor*, *at* http://www.export.gov/safeharbor/ (last visited May 5, 2005) [hereinafter Welcome to the Safe Harbor]. *See also* discussion *infra* Part I.B.

[12] *Id.*

[13] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 23 (1998).

[14] HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 36 (1999) (noting that France, Germany, and Great Britain all enacted privacy regulations in the 1970s).

[15] SWIRE & LITAN, *supra* note 13, at 23 (quoting FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32–33 (1997)).

[16] *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 199 n.16 (1992).

[17] *Id.*

[18] David Scheer, *For Your Eyes Only: Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL ST. J., Oct. 10, 2003, at A1.

1995, Germany, along with other countries, called on the European Commission for regulation.[19]

1. The European Data Protection Directive

For purposes of electronic transfers of private information, the primary modern EU rule is the European Data Protection Directive, formally adopted on October 24, 1995, and expected to be implemented by the Member states within three years.[20] The Data Protection Directive was created to harmonize data protection law throughout the EU.[21] It was an outgrowth of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[22] which resulted in "Guidelines on the Protection of Privacy and Transborder Flow of Personal

---

[19] *Id.*

[20] *Id.*; EDIRECTIVES: GUIDE TO EUROPEAN UNION LAW ON E-COMMERCE 121 (Arno R. Lodder & Henrik W.K. Kaspersen eds., 2002) [hereinafter EU E-COMMERCE LAW]. In January 2000, the European Commission took legal action against member states (France, Luxembourg, the Netherlands, Germany, and Ireland) that did not pass national laws to incorporate the data protection elements of the Directive as required. *See* Press Release, European Union, Data Protection: Commission Takes Five Member states to Court (Jan. 11, 2000), *available at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/00/10&format=HTML&aged=1&language=EN&guiLanguage=en; *see also Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data*, http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm (last visited May 5, 2005) (providing a current listing of the relevant laws of the member states and their status).

[21] Data Protection Directive, *supra* note 3, ¶¶ 7–8, at 31–32.

> Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member states may prevent the transmission of such data from the territory of one Member state to that of another Member state; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions.

Id. ¶ 7, at 31–32.

[22] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS No. 108 (Jan. 28, 1981), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm; *see also* EU E-COMMERCE LAW, *supra* note 20, at 119–20.

Data."[23] Those guidelines went into effect on September 23, 1980.[24] However, new technologies eroded the protections of those guidelines, and though the Organisation for Economic Co-operation and Development is working on a more modern treatment, the European Union developed the Data Protection Directive as a framework for data protection that covered the European Union nations.[25]

A directive, contrasted with a regulation, is by definition an "instruction" to European Union Member states to codify the directive's requirements within their national laws in the designated timeframe.[26] An important aspect of the Data Protection Directive is the obligation that each member state establish a "public authority" or agency to administer the Directive's requirements.[27]

The Data Protection Directive, like most European Union regulation, focuses on private sector data transfers—governmental uses and transfers of data are beyond the scope of its jurisdiction.[28] In deference, Article 13 of the Data Protection Directive offers exemptions to data involved in national security or public security; crime prevention, criminal investigation, detection or prosecution; the economic or financial interest of member states or the EU; "the exercise of official authority" in regards to the previous; and the protection of the individual or of "rights and freedoms of others."[29]

The source of privacy protection from which the Data Protection Directive emanates is the Charter of Fundamental

---

[23] Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (adopted Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited May 5, 2005).

[24] *Id.*

[25] *See* EU E-COMMERCE LAW, *supra* note 20, at 119–20.

[26] Simon Smith, *European Data Privacy Rights Not So Scary After All*, E-COMMERCE L. & STRATEGY, Mar. 13, 2003, at 3.

[27] Data Protection Directive, *supra* note 3, art. 28, at 47; *see also* KUNER, *supra* note 10, at 13–16 (discussing the breadth of duties of the agencies).

[28] SWIRE & LITAN, *supra* note 13, at 7.

[29] Data Protection Directive, *supra* note 3, arts. 13(1)(a)–(g), at 42. The Directive does not limit what member states may include within their criminal codes. JOEL R. REIDENBERG & PAUL M. SCHWARTZ, ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY: REGULATORY RESPONSES 141–42 (1998).

Rights of the European Union's[30] Article 8, which makes the protection of personal data an explicit right held by the individual and lays out a bar for legitimate need to access the data.[31] To put the protection of Article 8 into context, it is important to note that the first article discusses the inviolability of human dignity.[32] The subsequent Articles, 2–7, are titled, respectively, Right to Life, Right to the Integrity of the Person, Prohibition of Torture and Inhuman or Degrading Treatment or Punishment, Prohibition of Slavery and Forced Labour, Right to Liberty and Security, and Respect for Private and Family Life.[33] As part of this framework, the Data Protection Directive attempts to find balance between privacy and the desires for economic growth, recognizing that in a strong EU marketplace, "the free movement of goods, persons, services and capital . . . require[s] not only that personal data should be able to flow freely from one member state to another, but also that the fundamental rights of individuals should be safeguarded."[34]

2. Other Related EU Regulations

Apart from the Data Protection Directive, the topic of data protection was also addressed in the Telecommunications Data Protection Directive[35] and the Directive on Electronic

---

30 Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.

31 Protection of personal data[:]

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Id. art. 8, at 10.

32 *Id.* art. 1, at 9.

33 *Id.* arts. 2–7, at 9–10.

34 Data Protection Directive, *supra* note 3, ¶ 3, at 31.

35 Council Directive 97/66/EC of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 24) 1.

Commerce.[36] The Telecommunications Data Protection Directive applied the principles of the Data Protection Directive to the telecommunications sector, but its limitations[37] caused its repeal and replacement by Directive 2002/58/EC on Privacy and Electronic Communications ("Directive on Privacy and Electronic Communications").[38] The Directive on Privacy and Electronic Communications covers communication on public networks and contains security and confidentiality provisions that relate to information being transferred over electronic networks within the EU.[39] In addition, the Directive also delimits how cookies may be set on computers, restricts how mobile phone location information can be used and bans SPAM within the EU.[40] Notwithstanding these restrictions, the Directive on Privacy and Electronic Communications contains language suggesting its support of international commerce, communication, and the inevitable growth of electronic transmissions: "[t]he successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk."[41]

Meanwhile, the Directive on Electronic Commerce combines consumer protection elements with the encouragement of business,

---

[36] Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L 178) 1 [hereinafter Directive on Electronic Commerce]. For more information on these directives and their histories, see EU E-COMMERCE LAW, *supra* note 20, at 67–93, 119–45; Smith, *supra* note 26.

[37] *See generally* Abu Bakar Munir and Siti Hajar Mohd Yasin, *Retention of Communications Data: A Bumpy Road Ahead*, 22 J. MARSHALL J. COMPUTER & INFO. L. 731, 732-35 (2004). "[The Telecommunications Privacy Directive] imposed wide-ranging obligations on carriers and service providers to ensure the privacy of users' communications, including Internet-related activities. It covered areas that, until then, had fallen between the cracks of data protection laws." The Directive erred on the side of privacy for individuals, but after the Sept. 11 terrorist attacks in New York member countries expressed concern that the Directive could limit law enforcement agencies' access to suspect's communication records. *Id*. at 732.

[38] Council Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), ¶ 4, 2002 O.J. (L 201) 37 [hereinafter Directive on Privacy and Electronic Communications].

[39] *See generally id.*; *New European Privacy Rules Go into Effect*, COMPUTER & INTERNET LAW., Jan. 2004, at 21.

[40] *Id.*

[41] Directive on Privacy and Electronic Communications, *supra* note 38, ¶ 5, at 37.

but steers clear of discussions of personal data protection.[42] It covers business-to-business and business-to-consumer commerce.[43] Like the Data Protection Directive, it discusses the potential abuses by Internet service providers and other possible intermediaries in the transmission of data.[44] In Article 16, the Directive on Electronic Commerce encourages the formation of self-regulating trade associations "representing consumers in the drafting and implementation of codes of conduct affecting their interests."[45]

These directives act in consort with the Data Protection Directive.[46] Detailed treatment of the Data Protection Directive, which has seventy-two recitals and thirty-four articles, is beyond the scope of this Comment.[47]

3. Defintions in the Data Protection Directive

The definitions set out in the Data Protection Directive are crucial to understanding the *Lindqvist* decision and the United States' Safe Harbor provisions. The definitions offer insight into the Directive's scope and the ambiguities faced by those trying to follow its tenets.

Personal data comprises "any information relating to an identified or identifiable natural person."[48] The concept of identifiable includes "reference to an identification number or to one or more factors specific to his physical, physiological, mental,

---

[42] *See* TERRY R. BRODERICK, REGULATION OF INFORMATION TECHNOLOGY IN THE EUROPEAN UNION 76–77 (2000) (explaining how the Directive regulates certain "economic activities," but does not apply to "protection of personal data").

[43] Simon G. Zinger, *Current Issues in eCommerce: Regulation of Electronic Commerce in Europe: A Corporate Counsel Guide*, 19 ACCA Docket 40, 47 (2001).

[44] *Id.*

[45] Directive on Electronic Commerce, *supra* note 36, art. 16(2), at 14.

[46] *See generally* EU E-COMMERCE LAW, *supra* note 20.

[47] *See generally* Data Protection Directive, *supra* note 3. For a discussion of the Directive that predates the agreements between the EU and the U.S. Department of Commerce, see Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L. REV. 661 (1999). For a more detailed treatment, see EU E-COMMERCE LAW, *supra* note 20, at 119–20.

[48] Data Protection Directive, *supra* note 3, art. 2(a), at 38.

economic, cultural or social identity."[49] Article 2 of the Data Protection Directive contains one of the elements of the Directive that has raised great concern; the definition of processing, which:

> shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[50]

One commentator wrote that "[i]t is pretty clear that just about anything that could conceivably be done with data is covered by the term processing."[51] Another observed that "processing," is so broad that "[t]he Directive could have far-reaching effects on business practices within the United States and other 'third countries.'"[52] The multinational corporation, with large amounts of personal data stored in a variety of locations about both employees and customers, the e-commerce portal of any size whose products appeal to people throughout the world and the company using other companies in other countries to process data or payment or host the storage of data are all enterprises with activities and data covered by the Data Privacy Directive if that data refers to a European Union resident.[53] The risks could be high for large companies with decentralized or outsourced data collection and storage.[54] As companies attempt to reduce information technology costs by outsourcing offshore or using offsite storage, they can run into issues with the Directive.[55]

---

[49] *Id.*

[50] *Id.* art. 2(b), at 38.

[51] Smith, *supra* note 26.

[52] SWIRE & LITAN, *supra* note 13, at 3.

[53] *Cf.* Scheer, *supra* note 18. For example, General Motors' locations could not publish and distribute telephone books with European employee office numbers, as even office numbers are considered personal information, without the consent of the employees and adherence to other regulations. *Id.*

[54] *Id.*

[55] *Cf id.* Some companies are following the European lead, the "gold standard," according to DuPont's corporate counsel. DuPont has been seeking signatures on

4. The Issues of Third Country Transfers and "Adequate" Protections

The regulations concerning third country data transfers are important for the international economy.[56] Article 25 covers the transfer to third countries: "The Member states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place *only if . . . the third country in question ensures an adequate level of protection.*"[57] Adequacy "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations," and the type and use of the data.[58] In addition,

> 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.[59]

The many attributes which must be considered and the ongoing evolution of the meaning of "adequacy" in the European Union, as well as the interplay of country-by-country interpretation of Data Protection Directive, set the stage for some short-term uncertainty.[60]

B. The United States' Response to the Data Protection Directive: Safe Harbor

consent forms from employees and contracts with partners that state they will protect data they encounter. *Id.*

[56] *See* Reidenberg, *supra* note 5, at 1350–51.

[57] Data Protection Directive, *supra* note 3, art. 25(1), at 45 (emphasis added).

[58] *Id.* art. 25(2), at 45. An interpretation of the meaning of transfer was one of the things to come out of the *Lindqvist* decision. *See* discussion *infra* Part III.

[59] *Id*. art. 25(2), at 45.

[60] Reidenberg, *supra* note 5, at 1351.

The United States does not have a singular, cohesive national law on electronic privacy protection[61] and comes from a tradition of addressing individual needs rather than general principles for privacy regulations.[62] This section will address how the U.S. responded to the European Union's Data Protection Directive, by negotiating with E.U. regulators to establish the Safe Harbor guidelines to satisfy the Directive.[63]

With the segregated nature of the U.S.' treatment of data privacy, the U.S. did not meet the EU Data Protection Directive's requirement that any country where Member Country residents' data would be transferred must have "adequate" national law protection.[64] In response, the U.S. Department of Commerce negotiated the Safe Harbor principles with the EU authorities.[65]

---

[61] *See id.* at 1333, 1335.

[62] *See id.* at 1345–46; *see also* Joel R. Reidenberg, *Data Protection Law and the European Union's Directive: The Challenge for the United States, Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995) ("Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector. Legal rules have developed on an ad hoc, targeted basis, while industry has elaborated voluntary norms and practices for particular problems."); Scheer, *supra* note 18.

[63] Safe Harbor Overview, *supra* note 7.

[64] *See* Data Protection Directive, *supra* note 3, ¶¶ 56–57, at 36–37.

> 1. The Member states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
>
> 6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Id. art. 25(1) & (6), at 45–46.

[65] Safe Harbor Overview, *supra* note 7.

> The safe harbor—approved by the EU in 2000—is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor will assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Directive.

Id.

The U.S.-EU Safe Harbor Data Privacy Accord was finalized in the summer of 2000.[66] "Certifying" to the Safe Harbor covers notice, choice, onward transfer, security, data integrity, access, and means of enforcement and recourse. Safe Harbor provisions require that the organization:

> (1) informs users what information it collects and why,
>
> (2) lets the user opt out (and in some instances requires that the user opts in),
>
> (3) addresses the passing along to another organization or agent of the data,
>
> (4) permits the information to be accessible by the individual for correction or deletion,
>
> (5) "take[s] reasonable precaution" in regard to protecting data from "loss, misuse and unauthorized access, disclosure, alteration and destruction,"
>
> (6) ensures that data collection should be compatible with the use and takes "reasonable steps" regarding its reliability and accuracy, and
>
> (7) be subject to enforcement and recourse methods.[67]

The negotiated Safe Harbor provisions ensure that (1) if a U.S. firm is charged with a violation of EU privacy laws, then all member states will be bound by the European Commission's finding of "adequacy" of data protection, (2) requirements of pre-approval for data transfer will be granted or waived, and (3) claims brought by EU citizens will generally be heard in the United States.[68] The concept of "adequacy" was directly addressed in Commission Decision 2000/520/EC, which affirms that the United States' Safe Harbor principles may meet the bar for adequate

---

[66] Welcome to the Safe Harbor, *supra* note 11.

[67] *See* U.S. Dep't of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited May 5, 2005).

[68] Safe Harbor Overview, *supra* note 7.

protection.[69] The distinction between the United States' and European Union's treatment of data protection has been called the difference between "market mechanisms" and "state regulation."[70] The *Lindqvist* case illustrates those distinctions clearly and demonstrates state regulation at the extreme.

II. ISSUES RAISED IN THE *BODIL LINDQVIST* CASE AND SUBSEQUENT DECISION

The first ruling interpreting the EU Data Protection Directive came from a case originating in Sweden that tested the balance between privacy and the power of the free Internet.[71] *Case C-101/01 Criminal Proceedings against Bodil Lindqvist* arose after Lindqvist, who was a church maintenance worker and volunteer, took a computer class[72] and created some web pages with a variety of information about herself, her husband, and eighteen other church volunteers without their permission.[73] The web pages, created in late 1998, "included some full names, telephone numbers and references to hobbies and jobs held by her

---

[69] Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, art. 1, 2000 O.J. (L 215) 7.

[70] *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, 6 (2000).

[71] *Global Internet's Fragmentation by Govts., Innovation Debated*, WARREN'S WASH. INTERNET DAILY, Aug. 18, 2004. "'It is for the national authorities and courts responsible for applying the national legislation implementing the directive to ensure a fair balance between the rights and interests in question, including those fundamental rights,' such as free expression." *Id.* (citing *Lindqvist Judgment*, *supra* note 2).

[72] Peter Hitchens, *The Superstar Footballer, A Swedish Lady's Injured Foot . . . And a Sinister Threat to Our Freedom,* THE MAIL ON SUNDAY (London), Jan. 11, 2004, at 54.

[73] *See Lindqvist Judgment*, *supra* note 2, ¶¶ 12–14 (noting that Lindqvist originally set up her web page, which was linked to the Church's website, to provide information for parishioners making Confirmation); Jacqueline Klosek, *European Court Establishes Broad Interpretation of Data Privacy Law*, METROPOLITAN CORP. COUNS., Mar. 2004; *see also* Dan Tench, *You Can't Print That*, THE GUARDIAN (London), Jan. 5, 2004, at 10 (noting, though, that only sixteen other parishioners were included on the website).

colleagues,"[74] as well as information about one person's foot injury.[75] The pages also had information about preparing to take Communion at the church.[76]

Lindqvist was asked to remove the pages, which accounts describe as "gossipy,"[77] and written in a "mildly humorous manner."[78] She did so, but the Swedish data protection authorities nevertheless filed a complaint against her.[79] Lindqvist was charged with having:

> [1] processed personal data by automatic means without giving prior written notification to the Datainspektionen . . .; [2] processed sensitive personal data (injured foot and half-time on medical grounds) without authorisation . . .; [and] [3] transferred processed personal data to a third country without authorization. . . .[80]

Lindqvist was found guilty, fined approximately $500 and required to contribute to a fund for crime victims.[81] Part II will review the questions sent to the European Court of Justice, and then consider whether the decision gives guidance, concluding with a discussion of the meaning of "transfer" as suggested in the case.

A. The Questions the Swedish Court Sent to the European Court of Justice.

Bodil Linqvist agreed with the facts of the case during her trial in the district court (the Eksjö tingsrätt), but disputed her guilt and

---

74 Hitchens, *supra* note 72; *see also* Andre Fiebig, *The First ECJ Interpretation of the Data Privacy Directive*, MONDAQ BUSINESS BRIEFING, Dec. 2, 2003, *available at* 2003 WLNR 10746524.

75 *Lindqvist Judgment*, *supra* note 2, ¶ 13.

76 *See id*. ¶ 86.

77 Hitchens, *supra* note 72.

78 *Lindqvist Judgment*, *supra* note 2, ¶ 13.

79 *See id.* ¶ 15. Lindqvist failed to "notify the Datainspektionen . . . the supervisory authority for the protection of electronically transmitted data." *Id.* ¶ 14; *see also* Klosek, *supra* note 73; Mark Webber, *International Privacy Law Developments*, *in* FIFTH ANNUAL INSTITUTE ON PRIVACY LAW 2004: NEW DEVELOPMENTS & COMPLIANCE ISSUES IN A SECURITY-CONSCIOUS WORLD 313 (PLI 2004).

80 *Lindqvist Judgment*, *supra* note 2, ¶ 15.

81 Klosek, *supra* note 73; *see also* Webber, *supra* note 79, at 313.

appealed the district court decision.[82] The Göta hovrätt, the Swedish court of appeals, was unsure of the ramifications of the Data Protection Directive and hence the application of European Union law on several aspects of the case. They stayed the proceedings and requested guidance from the European Court of Justice.[83] The Göta hovrätt posed seven questions to the European Court of Justice regarding how the meaning of the Directive should be interpreted.[84] Part II.A of this Comment will consider the questions and the associated commentary by those submitting briefs and by the court.

1. On the Issue of "Processing"

The Göta hovrätt's first question addressed whether mentioning someone on an Internet page falls within the Data Protection Directive's scope, and if so, "[d]oes it constitute the processing of personal data wholly or partly by *automatic* means to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies."[85] This question, regarding the factual meaning of "processing," greatly concerns "third country" data collectors.[86] Lindqvist submitted that it was "unreasonable" that the "mere mention by name of a person or of personal data in a document" would constitute processing.[87] The Swedish government, conversely, claimed that processing under the Data Protection Directive includes "all processing in computer format."[88] The Commission of the European Communities asserted, "making personal data available on the internet constitutes processing wholly or partly by automatic means, provided that there are no technical limitations which restrict the processing to a purely manual operation. Thus, by its very nature, an Internet page falls within the scope of Directive 95/46."[89] The relevant article of the Directive, Article 3(1), states

82 *See Lindqvist Judgment*, *supra* note 2, ¶ 16.
83 *See Id.* ¶ 18; Klosek, *supra* note 73.
84 For a reproduction of the questions posed to the Court, see *infra* App. 1.
85 *Lindqvist Judgment*, *supra* note 2, ¶ 18(1) (emphasis added).
86 *Cf.* Smith, *supra* note 26.
87 *Lindqvist Judgment*, *supra* note 2, ¶ 20.
88 *Id.* ¶ 21.
89 *Id.* ¶ 23.

that "[t]his Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[90] In response to this issue, the ECJ found that:

> the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46.[91]

2. If Not Processing by Automatic Means . . .

The second question was only to be addressed if the first question was answered in the negative – that is, if the ECJ found that the "mention of a person . . . on an internet home page [is] an action" *outside* the scope of the Directive, and if the listing of the other church members were *not* considered to comprise some level of processing.[92] The Göta hovrätt, in the event the first question was answered in the negative, asked the ECJ if the

> act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute the processing *otherwise than by automatic means* of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1) of Directive 95/46.[93]

This question asks whether the activities in the *Lindqvist* case—if they do not consist of "processing of personal data wholly or partly by automatic means"—instead could be considered to fall

---

[90] Data Protection Directive, *supra* note 3, art. 3(1), at 39.

[91] *Lindqvist Judgment*, *supra* note 2, ¶ 27.

[92] *Id.* ¶ 18(1), (2). Processing in ¶ 18(1) is either "wholly or partly by automotive means."

[93] *Id*. ¶ 18(2) (emphasis added).

under the filing system component of Article 3(1).[94] Because the ECJ found that the creation of the Internet pages did fall under the scope of the Directive as defined in the first case of Article 3(1), it did not address whether or not they fell under the second.[95]

Considering, *arguendo*, that the Court needed to address Article 3(1)'s second case, the ECJ might have helped clarify some of the ambiguity surrounding the Directive's scope; the definitions section of the Directive gives little true guidance to what would be considered a "filing system," saying merely that a "'personal data filing system' . . . shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis."[96]

3. Did This Activity Fall under One of The Article 3(2) Exceptions?

The next question the European Court of Justice addressed in the decision was whether the facts at hand could possibly fall under exceptions in Article 3(2) of the Data Protection Directive exempting "processing of personal data . . . by a natural person in the course of a purely personal or household activity."[97] *Lindqvist* raised the issue of freedom of expression, claiming that those "creat[ing] internet pages in the course of a non-profit-making or leisure activity are not carrying out an economic activity and are thus not subject to Community law."[98] The Court called

---

94 Data Protection Directive, *supra* note 3, art. 3(1), at 39.

95 *Lindqvist Judgment*, *supra* note 2,. ¶ 28.

96 Data Protection Directive, *supra* note 3, art. 2(c), at 38.

97 *Id*. art. 3(2) at 39:

> This Directive shall not apply to the processing of personal data:
> - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
> - by a natural person in the course of a purely personal or household activity.

Id.

98 *Lindqvist Judgment*, *supra* note 2, ¶ 30.

Lindqvist's activities "charitable and religious,"[99] but said that, in addition to covering activities of the state (in defense and public safety, for example), the exceptions of Article 3 were to be taken literally and to apply to the "activities . . . expressly listed there or which can be classified in the same category."[100] It held that the exceptions did not apply to the "charitable and religious" activities, but rather applied to the "exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses."[101] Moreover, the ECJ held that the exception of Article 3 applied to "activities . . . carried out in the course of private or family life of individuals"[102] and not to "publication on the internet so that those data are made accessible to an indefinite number of people."[103] The Court said that the information Lindqvist published was not within the realm of the exceptions.[104]

In its comments to the Court, the Commission of the European Communities made several interesting arguments, suggesting that the interpretation of the exceptions listed in the Directive may be the grounds for further discussion.[105] The Commission asserted that the aim of the Directive was "to regulate the free movement of personal data in the exercise not only of an economic activity, but also of social activity in the course of the integration and functioning of the common market,"[106] and that to interpret otherwise "might entail serious problems of demarcation,"[107] especially insofar as the possibility of "pages containing personal data intended to disparage certain persons with a particular end in view might then be excluded from the scope of that directive."[108]

4. Did the Data Concern Health?

---

99 *Id.* ¶ 39.
100 *See id.* ¶ 44.
101 *Id.* ¶ 46.
102 *Id.* ¶ 47.
103 *Id.*
104 *See id.* ¶ 48.
105 *See id.* ¶¶ 30–36.
106 *Id.* ¶ 35.
107 *Id.* ¶ 36.
108 *Id.*

The fourth question the Göta hovrätt sent to the EJC was whether "reference" to a foot injury and to the fact that the injured person was working half-time on medical grounds "constitute[] personal data concerning health," as defined in Article 8(1) of the Directive.[109] The Court held that information regarding health—both mental and physical—should be given a "wide interpretation," and that the reference was clearly health information under the Directive.[110] Article 8 sets forth "special categories" of data, namely "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life."[111]

These types of information are not considered "special" in regards to processing, as far as the exceptions laid out in Article 8(2) are concerned. These exceptions include: when the person has "given . . . explicit consent,"[112] in employment law situations where allowed by national law and protected by "adequate safeguards,"[113] when "necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent,"[114] when the data is for legal claims,[115] or for "preventive medicine, medical diagnosis . . . or the management of health-care services, *and* where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy."[116] Additionally, the Directive explicitly allows for member state utilization of a universal identification number in this section.[117]

It is interesting to note that the Swedish authorities did not raise the question of whether information about the church volunteers, by naming them as church volunteers, also violated this

[109] *Id.* ¶ 49.
[110] *Id.* ¶ 50.
[111] Data Protection Directive, *supra* note 3, art. 8(1), at 40.
[112] *Id.* art. 8(2)(a), at 40.
[113] *Id.* art. 8(2)(b), at 40.
[114] *Id.* art. 8(2)(c), at 40.
[115] *Id.* art. 8(2)(e), at 41.
[116] *Id.* art. 8(3), at 41 (emphasis added).
[117] *Id.* art. 8(7), at 41.

sphere of "special categories" of data in regard to data about "religious or philosophical beliefs." Among the exceptions for use of "special category" information is one allowing for:

> processing . . . in the course of its legitimate activities with appropriate guarantees by a . . . non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.[118]

The facts of the *Lindqvist* case clearly indicate that the data subjects did not give their consent.[119]

5. Was There a "Transfer" of Data?

The fifth question referred by the Göta hovrätt addresses the meaning of "transfer" under Article 25 of the Directive.[120] "Transfer" is not defined within the Directive, either in the definitions section, Article 2, or in Chapter IV on the "Transfer of Personal Data to Third Countries."[121] Throughout the body of the Directive, however, transfer is used in discussions about moving data to third countries.[122]

The reference to the EJC specifically asked if there was a transfer of data in the construction of a web page, which was then stored as part of a site that could be visited by users from other

---

[118] *Id.* art. 8(2)(d), at 40–41.

[119] *See Lindqvist Judgment*, *supra* note 2, ¶ 14.

[120] *See id.* ¶ 52.

[121] Data Protection Directive, *supra* note 3, art. 2, at 38–39; arts. 25–26, at 45–46.

[122] The following are examples of instances where transfer is used to describe the moving of data to third countries: paragraphs 37 (on freedom of information); 56 (on international trade); 57 (on the adequacy of protection in third countries); 58 (on the need for exceptions to paragraph 57); 60 (on limiting transfers from member states only to third countries that are in compliance with the Directive); 66 (on making the Commission responsible for the implementation of a process for implementation of the Directive's components); Article 19 (regarding the notifications required to the member states about information being moved); and of course, Chapter IV, titled "Transfer of Personal Data to Third Countries" (covering in which cases and under what protections transfers outside of the EU can take place). *See id.* at 34–37, 44–46.

countries (including third countries).[123] Additionally, it questioned whether the lack of use of the page by third country residents or the hosting of the page in a third country would affect the response to whether data transfer had taken place.[124] In most of the other questions posed to the ECJ, the countries and the Commission of the European Communities, in submitting commentary, suggested reasoning and conclusions very much along the lines of the Court's decisions.[125] In their commentary regarding the fifth question, however, the Swedish government and the Commission state that putting data on the Internet "so that they become accessible to nationals of third countries, constitutes a transfer of data to third countries" under the Directive, even if there had been no third country call to the data.[126] The issue of data transfer was the third count on which Lindqvist was prosecuted in the lower Swedish courts; she "transferred processed personal data to a third country without authorization."[127] Transfer is used to discuss moving data from one state to another, as opposed to moving or presenting information from a server hosting web pages to a user's computer. The Court emphasized this distinction in its response to the question.[128]

The Court responded that in order to see Lindqvist's pages, a user would have to connect to the Internet and request the pages in question,[129] but that "Mrs[.] Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages."[130] The Court continued by emphasizing that Chapter IV of the Data Protection Directive makes no specific mention of the Internet:[131]

---

123 *See Lindqvist Judgment*, *supra* note 2, ¶ 52.

124 *See id.*

125 *See, e.g.*, *id.* ¶¶ 20–27.

126 *Id.* ¶ 53.

127 *Id.* ¶ 15.

128 *See id.* ¶¶ 59–71.

129 *See id.* ¶ 60.

130 *Id.*

131 *See id.* ¶ 67. "[I]t does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located." *Id.* Indeed, the term the "Internet" is not found anywhere in the body of the Directive. *See generally id.*

> one cannot presume that the Community legislature intended the expression transfer . . . to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.[132]

In its next Recital, the Court held that if transfer were equated to publication on the Internet, any publication of personal data on the Internet would be a transfer to all Internet-accessing third countries. Further, the Court held that if there were a singular Internet-accessing third country without adequate protection, then "Member states would be obliged to prevent any personal data being placed on the internet."[133]

6. Is Freedom of Expression Abridged?

The sixth question referred by the Göta hovrätt addressed whether, by the application of the Data Protection Directive to facts of the *Lindqvist* case, conflicts arise with freedom of expression or other fundamental rights.[134] The Court responded that the Directive is broad, thus covering many possible situations, but that the protection of fundamental freedoms—expression and the protection of individual privacy among them—are inherent in the text of the Directive.[135] The *Lindqvist* Court urged other courts in member states to apply proportionality in future questions and to use care so that neither member state law nor the Directive is interpreted in a manner that infringes on the freedom of expression.[136] As in this case "Mrs[.] Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the

---

[132] *Id.* ¶ 68.
[133] *Id.* ¶ 69. The United States would certainly be considered such a third country.
[134] *See id.* ¶ 72.
[135] *See id.* ¶¶ 79, 82.
[136] *See id.* ¶ 87.

individuals about whom Mrs[.] Lindqvist has placed data on her internet site."[137]

7. How Much Latitude Does a Member State Have in Privacy Legislation?

The seventh question referred by the Göta hovrätt asked whether a member state could have more restrictions than those found within the Directive.[138] This question strives to determine if the Directive is meant as baseline legislation or as a piece of harmonizing legislation.[139] The ECJ responded that member states may apply national legislation to areas beyond the scope of the Directive-based legislation as long as that extension is not prohibited by other Community law.[140] The ECJ further described the Directive's ambition as "harmonisation which is generally complete."[141] Analyzing Recital 10 of the Directive, the ECJ responded that the goal of the Directive is equivalence in the laws of the member states,[142] but that the Directive accords "a margin for [Member states to] manoeuvre in certain areas and authorises them to maintain or introduce particular rules."[143] The ECJ held that legislation "must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life."[144]

B. Does the Decision Offer Guidance or Cause More Confusion?

Lindqvist did not expect to lose the case.[145] "She . . . view[s] this as Big Brother gone mad. She sees this as an infringement of

---

[137] *Id.* ¶ 86.

[138] *See id.* ¶ 91.

[139] *Id.* ¶¶ 91–99. Once again, the Commission urges a somewhat different take on the matter in its comments to the Court: "The Commission therefore submits that a Member state cannot make provision for more extensive protection for personal data or a wider scope than are required under the directive." *Id.* ¶ 94.

[140] *Id.* ¶ 99.

[141] *Id.* ¶ 96.

[142] *Id.* ¶ 95.

[143] *Id.* ¶ 97.

[144] *Id.* ¶ 99.

[145] Hitchens, *supra* note 72.

her rights. She did this for a bit of fun and was hounded by parishioners and even the vicar," her lawyer told the press.[146] He said that she asked to be prosecuted as a test case.[147] The case offers an interesting framework for comparison between data protection in the United States and European Union. An action such as this would be highly unlikely in the United States without at least the perception of harm by some party.[148] In the United States, the party perceiving harm would seek to remedy that harm, generally as an individual with an equity or tort claim.[149] In contrast, the *Lindqvist* case emphasizes that the Data Protection Directive applies to information about individuals—individually, as opposed to large amounts of gathered information about a group of individuals—and offers those individuals a right of action.[150] That right of action is carried out on the behalf of the individual who claims a misuse of their information.[151]

C. What Is a Transfer?

Lindqvist is the first case on the questions of transfer to third country and whether creating Internet pages is, *per se*, a transfer.[152]

---

[146] *Id.* Lindqvist's lawyer, Sture Larsson, said, "She feels like the victim of a medieval witchhunt rather than a member of an advanced European society." *Id.*

[147] *Id.*

[148] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 963–64 (1989).

[149] There are also some cases in which state law could offer protection. *See* discussion *infra* Part III.B.4.

[150] *See generally Lindqvist Judgment*, *supra* note 2. "Member states shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question." Data Protection Directive, *supra* note 3, art. 22, at 45.

> 1. Member states shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
> 2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Id. art. 23, at 45.

[151] Data Protection Directive, *supra* note 3, art. 28, at 48 ("Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.").

[152] *Lindqvist Judgment*, *supra* note 2, ¶ 69.

In Recital 69 of the *Lindqvist* decision, the response to the question of the meaning of data transfer is unambiguous:

> If Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet.[153]

Hence, the implications of defining transfer as such would be stupendous and unwieldy. "[I]f the Commission found . . . that even *one* third country did not ensure adequate protection, the Member states would be obliged to prevent any personal data being placed on the internet," the decision continues.[154] Save the Safe Harbor provisions, the United States is considered such a third country, thus, it is fair to assume that there would at least be one third country with inadequate protection.

The Court enunciated, "it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as those carried out by Mrs. Lindqvist do not as such constitute a transfer [of data] to a third country."[155] But then, what meaning does "transfer" have within the Data Protection Directive?

> [T]here is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member state loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member state, thereby making those data accessible to anyone who connects to the internet, including people in a third country.[156]

So a transfer to a third country is not what the facts of the *Lindqvist* case state, nor is it making Internet pages that are hosted on servers in one's own or another European Union member

---

153 *Id.*; *see also* discussion *supra* Part I.A.4.
154 *Lindqvist Judgment*, *supra* note 2, ¶ 69 (emphasis added).
155 *Id.* ¶ 70.
156 *Id.* ¶ 71.

state.[157] This raises, but leaves unanswered, the issue of whether transfer takes place when information about EU residents, placed there by residents of EU member states, appears on Web pages hosted on servers in non-member countries.[158]

In the past, content on Web pages hosted in the U.S. has received foreign attention.[159] If such content included personal information about residents, it could, under the possibility raised above, draw the attention of the European Court of Justice. The Court has expressed a lack of interest in considering the possible access of Internet pages by third country residents;[160] this suggests

---

[157] *See id.* ¶¶ 69–71.

[158] *See id.* ¶ 70 ("It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country."). For a pragmatic discussion of what businesses need to do and how they need to approach the Data Protection Directive, see A BUSINESS GUIDE TO CHANGES IN EUROPEAN DATA PROTECTION LEGISLATION 25–124 (1999).

[159] In November 2000, a French judge, in a widely criticized opinion, told Yahoo! that French users had to be prevented from seeing pages on the U.S. version of the auction site that sold Nazi war memorabilia and neo-Nazi objects. Timothy D. Casey & Jeff Magenau, *A Hybrid Model of Self-Regulation and Governmental Regulation of Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1, 16–17 (2002). If the company did not comply, it would be heavily fined (about $14,000/day). *Id.* The items had been taken off the French Yahoo! sites. *Id*. at 17. French law "strictly prohibits the display or sale of objects that incite racial hatred." *See Yahoo!'s French Connection*, THE ECONOMIST, Nov. 20, 2000, http://www.economist.com/displayStory.cfm?Story_ID=431328 (last visited Apr. 25, 2005). The dispute has also been heard in U.S. courts, as Yahoo! sought declaration that the French ruling did not apply to the U.S. versions, but was told by the Ninth Circuit that Yahoo! could not assert a First Amendment right until the French organizations sought relief in U.S. courts. *See* Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 379 F.3d 1120, 1126 (9th Cir. 2004).

> The implications [of the French judge's decision] for e-commerce jurisdiction are significant, as businesses seeking to avoid regulation in a foreign country may be forced not only to refrain from purposefully directing prohibited content at nationals of the regulating country, but could actually be required to install protective measures to prevent nationals from a regulating country, even those speaking another language than their native tongue, from accessing a site not specifically directed at them.

Casey & Magenau, *supra*, at 17.

[160] *See Lindqvist Judgment*, *supra* note 2, ¶¶ 70–71; *see also* Taylor Wessing, *Bodil Lindqvist C-101/01*, *at* http://www.taylorwessing.com/topical/intellectual_property/1103_bodil.html (last visited May 5, 2005). The issue of transfer outside the context of Web pages has been an issue before the court, especially in the context of employment information being transferred from one office in the European Union to another corporate

to interested parties that the Court's definition of transfer has no dependencies on the location of the data from a technological point of view, nor is the Court interested in parsing distinctions about recipients of the data in the definition of transfer.

III. THE *LINDQVIST* DECISION IS NARROW, INADEQUATE, AND MISUNDERSTANDS THE REALITIES OF BUSINESS

Bodil Lindqvist was a private citizen who built Internet pages as homework for a class she was taking.[161] She was not involved in commerce nor was she collecting large amounts of data about individuals. Indeed, the actions that got her into trouble were geared toward enhancing her community and connecting with and serving fellow church members.[162] When she was asked to take down the pages, she acquiesced.[163] The facts of the case specify neither embarrassment on the part of the subjects of the pages nor any harm, economic or otherwise.[164] Yet the case came before the Swedish data protectors and was escalated.[165] The possibility of having each and every citizen claim that his or her privacy has been compromised by a use of information about him or her somewhere on the Internet is a monumental bureaucratic disaster, one which is it difficult to imagine was the imagined intent of the drafters of the European Union's Data Protection Directive.[166] In conclusion, Part III will address some of the breaches of personal data outside of the European Union, then review the existing law in the United States covering the protection of personal information, before concluding that U.S. lawmakers should use the *Lindqvist*

office, either within or outside the EU. A discussion of this is beyond the scope of this Comment.

[161] *See Lindqvist Judgment*, *supra* note 2, ¶ 2.

[162] *See id*. ¶ 12 (discussing how the original impetus behind Lindqvist's creation of her Web page was to provide information for fellow congregants who would be receiving Confirmation).

[163] *Id.* ¶ 14 ("She removed the pages in question as soon as she became aware that they were not appreciated by some of her colleagues."); Klosek, *supra* note 73.

[164] *See Lindqvist Judgment*, *supra* note 2, ¶¶ 13–14.

[165] *See* Klosek, *supra* note 73.

[166] *Id.* "The court's finding highlights the fact that Europe's data protection regime is extremely far reaching. The enforcement action that was launched against Lindqvist, and validated in large part, by the ECJ, is not likely to be the last of its kind." *Id.*

case as a warning of the sorts of poor decisions that can result from heavy-handed centralized legislation.

A. Breaches of Personal Information

The *Lindqvist* case is an extremely minor exposure of limited personal information. In contrast, breaches of security have affected customers of GMAC Insurance,[167] Equifax Canada,[168] and, in February 2005, at "data collection giant," ChoicePoint.[169] San Diego State University and Indiana State University have both experienced invasions that have compromised the security of employee and student information.[170] In all these cases, at least thousands of personal records were compromised.[171] Less than a month after the ChoicePoint compromise, a suit had already been filed seeking class status for those whose information was involved.[172] Compared to these actions, and the resulting potential damage to the financial security of those individuals involved, the condemnation by the European Court of Justice of Lindqvist's actions appears draconian and abusive.

The breaches in the United States, and the resulting outcry from consumers, have caused politicians to call for more cohesive laws governing data protection and punishing companies whose data is compromised.[173] But U.S, legislators should view the

---

[167] *See* George V. Hulme, *Breach of Trust*, INFORMATIONWEEK, May 3, 2004, at 58. GMAC Insurance had two laptops stolen with 200,000 records containing "Social Security numbers, home addresses, and credit scores," while Equifax Canada alerted more than 1400 people of a breach. *Id.* San Diego State alerted 178,000 about possible exposure during hackers' attack. *See id.* Meanwhile, nearly 145,000 people in Choice Point's systems had information including Social Security numbers and addresses passed to a con artist. Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1.

[168] *See* Hulme, *supra* note 167.

[169] Zeller, *supra* note 167.

[170] *See* Hulme, *supra* note 167.

[171] GMAC Insurance had two laptops stolen with 200,000 records containing "Social Security numbers, home addresses, and credit scores," while Equifax Canada alerted more than 1400 people of a breach. *Id.* San Diego State alerted 178,000 about possible exposure during hackers' attack. *See id.* Meanwhile, nearly 145,000 people in ChoicePoint's systems had information including Social Security numbers and addresses passed to a con artist. Zeller, *supra* note 167.

[172] Zeller, *supra* note 167.

[173] *Id.*

Lindqvist decision as a warning sign in the dangers of broadly legislating privacy. In the aforementioned breaches, the individuals whose information was exposed suffered harm, and that harm was suffered by more than one person.[174] To better understand the methods of remediating possible harm, it is first important to understand the major laws governing private information.

B. The Range of Privacy Regulations in the U.S. Currently

The U.S. Department of Commerce itself calls the U.S. approach a "sectoral . . . mix of legislation, regulation, and self regulation."[175] The legislation includes the Fair Credit Reporting Act, which addresses the use of credit reports and means for resolving disputes by consumers of the information contained within them;[176] the Driver's Privacy Protection Act, which states that motor vehicle agencies cannot release personal information about licensees;[177] the Privacy Act of 1974, which controls the information held on individuals by the government agencies and how it may be disclosed;[178] legislation on school records; workplace privacy laws, where the privacy rights afforded private and governmental employees are vastly distinct;[179] the law on the use of polygraphs;[180] and the law governing the disclosure of medical information;[181] to name just a few.[182]

---

[174] *Id.*

[175] Safe Harbor Overview, *supra* note 7. "The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin." *Id.*

[176] 15 U.S.C. § 1681 (2000).

[177] 18 U.S.C. § 2721 (2000).

[178] 5 U.S.C. § 552a (2000).

[179] Workplace privacy rights differ for the approximately three million U.S. federal employees and their private sector counterparts. DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 618–19 (2003). For a more detailed discussion of the protections afforded federal employees, see *id.* at 618–85.

[180] Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001 (2000).

[181] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified at 42 U.S.C.A. § 210 (2000)).

[182] For an overview of U.S. federal legislation on privacy, state counterparts, and cases involving privacy, see HENDERSON, *supra* note 14, at 40–85.

1. Protecting Children Online

The federal government has been particularly interested in protecting children online by attempting to protect their privacy and prohibiting them from seeing inappropriate content.[183] COPA and COPPA are oft-confused but different pieces of legislation with much history. The Child Online Protection Act ("COPA")[184] addressed marketing and obscenity that might be seen by children.[185] The Supreme Court has held, however, that COPA is likely unconstitutional in its interference with the protections of the First Amendment.[186] In contrast, the Children's Online Privacy Protection Act ("COPPA"),[187] an amendment to the Communications Act of 1934, is still viable.[188] COPPA, which is administered by the Federal Trade Commission ("FTC"), addresses the online collection of personally identifiable information about children (defined as those under 13).[189] It requires parental consent and information control when a website targeted to children collects personally identifiable information and limits the use of cookies and other tracking devices.[190]

---

[183] Much has been written about children and the Internet. *See, e.g.*, Ronald J. Krotoszynski, *Childproofing the Internet*, 41 BRANDEIS L.J. 447 (2003); Melanie Hersh, Note, *Is COPPA a Cop Out?: The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should Be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831 (2001).

[184] 47 U.S.C. § 231.

[185] 47 U.S.C. § 231

> Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

Id.

[186] Ashcroft v. ACLU, 124 S. Ct. 2783, 2789, 2795 (2004); Krotoszynski, *supra* note 183, at 453–55.

[187] 15 U.S.C.A. §§ 6501–06 (2000).

[188] *Id.*

[189] 15 U.S.C.A. § 6501(1).

[190] *See* Facts for Businesses, *How to Comply with the Children's Online Privacy Protection Rule*, *at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (last visited May 5, 2005).

> The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that

2. Protection of Health Information

Health information is generally less protected. "Our private health information [is] being shared, collected, analyzed, and stored with fewer federal standards than video store records," reported Donna E. Shalala, Secretary of Health and Human Services under the Clinton administration.[191] Some recourse does exist for the misuse and inappropriate processing of sensitive personal information in the U.S. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[192] was enacted primarily so that employees could more easily change jobs without being penalized by health insurance companies for pre-existing conditions, but it also included provisions for more protection of health information.[193] Nonetheless, emphasizing Shalala's point above, individuals incur responsibility only when associated with official functions in a medical office under HIPAA.[194]

3. Privacy as Consumer Protection

The FTC also has enforcement powers for privacy violations under the Gramm-Leach-Bliley Act.[195] The FTC's traditional consumer protection role is expanding as it takes an active interest

> would allow someone to identify or contact the child. The Act and Rule also cover other types of information—for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms—when they are tied to individually identifiable information.

Id.

[191] DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 65 (1998).

[192] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified at 42 U.S.C.A. § 210 (2000)).

[193] *See* SOLOVE & ROTENBERG, *supra* note 179, at 210.

[194] *Id.*

[195] Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.). Gramm-Leach-Bliley broadly covers financial institutions as well as brokerages, tax return preparations, financial advising companies, credit counseling and others. *See* Privacy Initiatives, *Financial Privacy: The Gramm-Leach Bliley Act*, *at* http://www.ftc.gov/privacy/glbact/index.html (last visited May 5, 2005); *see also* Mike Hatch, *Electronic Commerce in the 21st Century: The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1476 (2001).

in the prosecution of transgressions.[196] Indeed, the agency's website states that "[p]rivacy is a central element of the FTC's consumer protection mission."[197] "The Federal Trade Commission is educating consumers and businesses about the importance of personal information privacy, including the security of personal information."[198] For example, the FTC was involved in a controversy after the Internet retailer Toysmart declared bankruptcy and ran advertisements offering its database of customer information for sale.[199] The FTC came to an agreement with Toysmart for terms under which it could make the sale, an action disputed by the attorneys general of thirty-eight states.[200] In the end, the issue was moot, as an investor bought the database and destroyed the information within. Even so, the case raised issues about the many players with stakes in privacy disputes and data ownership.[201] It also may be considered an an example of how the "sectoral" approach can work in the United States, where despite controversy between them, government officials and the courts ended up with a just result.

As in Europe, personal privacy is a deep-rooted concern. There is some irony in the fact that Lindqvist's actions were viewed as "gossipy"[202] when one reflects back to the seminal Warren and Brandeis treaty on privacy, the adoption of which is believed to have been a response to an active press desperate for details about society.[203] The Warren and Brandeis treaty was rooted in concern about "intrusions into individual privacy by nineteenth century journalists armed with the latest technological innovations."[204] Though technology continually changes (it was the increasing use of newspaper photography that made those

[196] *See* Privacy Initiatives, *Introduction*, *at* http://www.ftc.gov/privacy/index.html (last visited May 5, 2005).
[197] *Id.*
[198] *Id.*
[199] Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 389 (2003).
[200] *See id.* at 390.
[201] *See id.*
[202] *See supra* text accompanying note 77; *see also* Hitchens, *supra* note 72.
[203] Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 703, 709 (1990).
[204] *Id.* at 703.

commentators pause),[205] the underlying concept of finding a right to action in tort remains the staple of law in the United States for damage to reputation.

4. The Tort of Violating Another's Privacy

Though the transfer or processing of data is not regulated in the United States,[206] a person who violates the privacy of another by creating a web page, for instance, could face liability for "the resulting harm to the interests of the other,"[207] generally under state law.[208] This invasion of privacy is generally understood to mean one of four invasions: "(a) unreasonable intrusion upon the seclusion of another, . . . (b) appropriation of the other's name or likeness, . . . (c) unreasonable publicity given to the other's private

[205] "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' " Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[206] In the United States, with limited exceptions, the processing and transferring of data per se is not among those activities that either the state or federal governments monitor. In the U.S., Lindqvist would not, either as an individual or a business, have been required to register with any entity before creating Web pages or even sending data from her location to others. If she had begun to operate as a business, she could have made the determination that she should apply for a privacy seal such BBBOnline (part of the Better Business Bureau. See http://www.bbbonline.org (last visited May 5, 2005)), TRUSTe (Founded by the Electronic Frontier Foundation, TRUSTe had 1413 websites carrying their seal as of Sept. 2004. *See* http://www.truste.org/about/fact_sheet.php (last visited May 5, 2005)) or WebTrust (See http://www.cpawebtrust.org/homepage.htm (last visited May 5, 2005). The WebTrust program is administered by the American Institute of Certified Public Accountants). Or she might decide to join a self-regulating organization such as the Direct Marketing Association, which would require her business to follow their best practices and offer complaining consumers a forum for their grievances on privacy violations. *See* http://www.the-dma.org/aboutdma (last visited May 5, 2005). And example of sectoral self-monitoring, the DMA has issued a "Privacy Promise" that it expects member organizations to follow in addition to business practice guidelines in several areas. *See* Direct Marketing Association Guidelines for Ethical Business Practice, at http://www.the-dma.org/guidelines/ethicalguidelines.shtml (last visited May 5, 2005). The Direct Marketing Association is the largest trade organization for business involved in "direct, database, and interactive global marketing." *See* http://www.dmaconsumers.org/privacy.html (last visited May 5, 2005).

[207] *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[208] For information on which forms of information are protected on a state-by-state basis, see http://www.epic.org/privacy/consumer/states.html (last visited May 5, 2005).

life, . . . or (d) publicity that unreasonably places the other in a false light before the public . . . ."[209] In *Lindqvist*, the veracity of the material is not discussed.[210] Assuming, *arguendo*, the information printed was not false, the closest tort question would be unreasonable publicity,[211] which generally requires that the publicity be of "a kind that . . . would be highly offensive to a reasonable person."[212]

CONCLUSION

The Swedish court found Lindqvist guilty of three counts: processing personal data by automatic means without notifying the authorities, the processing of sensitive personal data, and transfer of data to third countries.[213] The European Court of Justice said Lindqvist had not been guilty of a transfer, but that she was guilty of processing and that the data involved included health information.[214]

Lindqvist was clearly a test case of the Data Protection Directive, one that pushes many issues and muddies as much as it clarifies. As Lindqvist's lawyer stated, "This decision emphasises the wide-reaching and indiscriminate nature of the European Union's data protection laws."[215] He's not alone in thinking that the EU rules are short-sighted and may in the end stifle the businesses they claim to encourage. A study commissioned by the European Commission and executed by the United Kingdom-based

---

[209] RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[210] *See generally Lindqvist Judgment*, *supra* note 2.

[211] *See* RESTATEMENT (SECOND) OF TORTS § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy.").

[212] *Id.* § 652D(a).

> [A]nyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part. Thus he must expect the more or less casual observations of his neighbors as to what he does, and that his comings and goings and his ordinary daily activities, will be described in the press as a matter of casual interest to others.

Id. § 652D cmt. c.

[213] *See* discussion *supra* Part II.

[214] *See generally Lindqvist Judgment*, *supra* note 2. *See* also discussion *supra* Part II.

[215] Hitchens, *supra* note 72.

Consumers International casts doubt on the assertion of U.S. data protection inadequacy.[216] The five-year study of 751 websites in the United States and Europe, released in 2001, found that "[d]espite tight EU legislation . . . U.S.-based sites tend to set the standard for decent privacy policies."[217] It also found that eighty percent of European websites surveyed did not comply with EU data storage opt-out rules and only about one-third direct users to privacy policies, another EU requirement.[218] "The evidence is that enforcement [of the regulations] is simply not happening."[219] "When you talk to the national regulators who are supposed to make sure the rules are applied, they always complain of a lack of funding and a lack of staff for an enormous amount of work."[220] Meanwhile, in New York, the online arm of lingerie retailer Victoria's Secret agreed to a fine of $50,000 by Attorney General Eliot Spitzer for exposing the orders, names, and addresses of more than 560 customers.[221] "The consumer protection laws of the 1930s have become the privacy law of the 21st century," Spitzer told the New York Times.[222]

And so, in the United States, the debate continues about the various approaches: unified federal law on privacy, state laws, and the market-driven, self-regulating approach to privacy. "There may soon come a point when a business community will have to decide whether it prefers a single comprehensive federal rule, or a situation in which a variety of state rules create difficult-to-follow mandates," argued then-FTC Chairman Robert Pitofsky in a 2000 speech in Washington, D.C., questioning the self-regulation of the U.S. ecommerce industry.[223] From a U.S. business perspective, it

---

[216] *See* Ben Vickers, *Europe Lags Behind U.S. on Web Privacy*, WALL ST. J., Feb. 20, 2001, at B11I.

[217] *Id.*

[218] *Id.*

[219] *Id.* (quoting Anna Fielder, Director of Consumers International in London).

[220] *Id.*

[221] John Schwartz, *Victoria's Secret Reaches a Data Privacy Settlement*, N.Y. TIMES, Oct. 21, 2003,
at C14.

[222] *Id.*

[223] Glenn R. Simpson, *FTC Chief Says E-Commerce Industry Should Reconsider Privacy-Rules Stance*, WALL ST. J., Feb. 11, 2000, at B3. Deborah Platt Majoras was sworn in on August 16, 2004, as Chairman of the Federal Trade Commission. For the

is difficult to fathom the potential chaos and confusion from a national law like the Data Protection Directive.

The conclusions reached in the *Lindqvist* case, especially as the Web pages she created were not considered to be part of "household" activities, are difficult to imagine even amid our litigious and highly regulatory-prone U.S. climate; the wide reach of the European Court of Justice seems contrary to some forms of community building in our open society. Additionally, the sixth question addressed to the ECJ—whether freedom of expression would be hindered by finding that Lindqvist violated the Directive—it seems possible that the suppression of more controversial information or discussion, for example the location of radioactive waste sites, the addresses of convicted sex offenders, or the salaries of high-level government employees, might have been found to violate freedom of expression. The implications for bloggers, the Internet diarists whose commentary increasingly finds its way into the mainstream media, are considerable. But on both sides of the Atlantic, it likely will take more cases like the *Lindqvist* decision and more near-misses such as the *Toysmart* settlement before the issues are settled.

The United States Department of Commerce did a disservice to businesses transacting with the residents of the European Union in agreeing to the Safe Harbor provisions. The "self-certification" process is effectively meaningless and tedious for the companies who attempt it, and allows the flaws of the European Union's Data Protection Directive to find their way into the much more responsive and agile system in the United States.

text of Majoras's speeches, see *Speeches/Articles by Deborah Platt Majoras, Chairman*, http://www.ftc.gov/speeches/majoras.htm (last updated May 9, 2005).

Appendix 1 – Questions sent to the European Court of Justice

Recital 18 of Case 101/01, *Criminal proceedings against Bodil Lindqvist*[224]

18. As it had doubts as to the interpretation of the Community law applicable in this area, inter alia Directive 95/46, the Göta hovrätt decided to stay proceedings and refer the following questions to the Court for a preliminary ruling:

(1) Is the mention of a person—by name or with name and telephone number—on an internet home page an action which falls within the scope of [Directive 95/46]? Does it constitute the processing of personal data wholly or partly by automatic means to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies etc.?

(2) If the answer to the first question is no, can the act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1)?

If the answer to either of those questions is yes, the hovrätt also asks the following questions:

(3) Can the act of loading information of the type described about work colleagues onto a private home page which is none the less accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?

(4) Is information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds personal data concerning health which, according to Article 8(1), may not be processed?

---

[224] *Lindqvist Judgment*, *supra* note 2, ¶ 18.

(5) [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden—with the result that personal data become accessible to people in third countries—does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?

(6) Can the provisions of [Directive 95/46], in a case such as the above, be regarded as bringing about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined in inter alia Article 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms?

Finally, the hovrätt asks the following question:

(7) Can a Member state, as regards the issues raised in the above questions, provide more extensive protection for personal data or give it a wider scope than the directive, even if none of the circumstances described in Article 13 exists?