

3-1-1999

## A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Control

Michael W. Heydrich

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/bjil>

---

### Recommended Citation

Michael W. Heydrich, *A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Control*, 25 Brook. J. Int'l L. (1999).

Available at: <https://brooklynworks.brooklaw.edu/bjil/vol25/iss2/27>

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of International Law by an authorized editor of BrooklynWorks.

# NOTES

## A BRAVE NEW WORLD: COMPLYING WITH THE EUROPEAN UNION DIRECTIVE ON PERSONAL PRIVACY THROUGH THE POWER OF CONTRACT

### I. INTRODUCTION

The old adage "knowledge is power"<sup>1</sup> has been professed throughout the ages. However, never before in history has the ability to accumulate, manipulate and disseminate information existed on the scale it does today.<sup>2</sup> In recent years, information of the most personal nature<sup>3</sup> can be accessed through scientific breakthroughs such as DNA testing<sup>4</sup> and distributed globally via the Internet. The tremendous impact on society of

---

1. Attributed to Frances Bacon, *Med. Sacrae: de Haeresibus*. See M. FRANCES MCNAMARA, 2000 CLASSIC LEGAL QUOTATIONS 330 (1992).

2. Based on a 1994 estimate, computers in the United States alone hold five billion records, trading information on every individual at an average of five times per day. The credit industry accounts for 400 million files which are updated by more than two billion entries every month in order to make possible 1.5 million credit decisions daily. See FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 2 (1997). See also Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591 (1994).

3. See Frederic Golden, *Good Eggs, Bad Eggs*, TIME, Jan. 11, 1999, at 58.

4. *Id.* Some of the genetically linked disorders that can currently be detected through DNA testing are: cystic fibrosis, Down's Syndrome, Duchenne muscular dystrophy, hemophilia A, Huntington's disease, polycystic kidney disease, and Tay-Sachs disease. See also KENNETH STARR, *THE STARR REPORT: THE OFFICIAL REPORT OF THE INDEPENDENT COUNSEL'S INVESTIGATION OF THE PRESIDENT* 57 (1998). DNA testing was used to determine that the residue on Monica Lewinski's dress was President Clinton's sperm. According to the report, "the genetic markers on the semen, which match the President's DNA, are characteristic of one out of 7.87 trillion Caucasians." *Id.* In the absence of DNA testing the President's sexual relationship with Ms. Lewinski would have been very difficult to prove, while the DNA results left no doubt. This is a prime example of how technology affects the privacy of even the most powerful persons in society. *Id.*

this superior accessing and distribution ability was recently most readily observed by the rapid availability of the Starr Report<sup>5</sup> and President Clinton's Grand Jury testimony on videotape over the Internet. While such technological advances are indeed a goal for which to strive, these same advances add urgency to the establishment of adequate safeguards for ensuring the privacy of individuals.

The need for privacy has been recognized by the public<sup>6</sup> and addressed to varying degrees by the governments of the European Union Member countries<sup>7</sup> and the United States.<sup>8</sup> Of specific concern has been the protection of personal data. With the capacity to convert data into binary form,<sup>9</sup> the ability

5. STARR, *supra* note 4.

6. The issue of privacy has been discussed in such literary works as George Orwell's *Nineteen Eighty-Four*, (depicting control of the public by the government by virtue of the government's censorship power and constant scrutiny of individuals which denied them the power for self-expression), GEORGE ORWELL, *NINETEEN EIGHTY-FOUR* (1949), and cinematic works like *Brazil* (showing subjugation of the public to government control by means of governmental control of all information), *BRAZIL* (Universal Pictures 1985), and *Gattaca* (depicting genetic testing being performed on everyone, and denying of opportunities to achieve their potential to those with an inferior genetic makeup), *GATTACA* (Columbia Pictures 1997).

7. For example, Belgium, France, Great Britain, Sweden, and West Germany already had promulgated various privacy laws. See Patrick E. Cole, *New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws*, 17 N.Y.U. J. INT'L L. & POL. 893, 902-08 (1985).

8. In the United States the notion of the right to privacy, or the right to be "let alone" dates back to the 19th century, and already appeared in a torts treatise at that time, THOMAS M. COOLEY, *A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT* 29 (2d ed., Chicago, Callaghan & Co., 1888). The right to be "let alone" as a component of privacy law, however, received publicity through the publication of the now famous *The Right to Privacy* law review article by Samuel D. Warren and Lois D. Brandeis. See Samuel D. Warren & Lois D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). See also PAUL SCHWARTZ & JOEL REIDENBERG, *DATA PRIVACY LAW* 37 (1996). Although there is no right to privacy mentioned specifically in the United States Constitution, the Supreme Court has derived that right from the substantive due process clauses of the 5th and 14th Amendments in such seminal cases as *Roe v. Wade*, 410 U.S. 113 (1973), *Griswold v. Connecticut*, 381 U.S. 479 (1965), and *Pierce v. Society of Sisters*, 268 U.S. 510 (1925). The Court has further strengthened this concept in *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977), identifying two elements of informational privacy: an "individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions." See SCHWARTZ & REIDENBERG, *supra*, at 76, 82-83.

9. Binary form is the conversion of data to its simplest form where all data is expressed as either zeroes and ones or as ON/OFF. The reduction to a two state (or binary form) makes it possible to store information on optical or magnetic media by magnetizing/demagnetizing sections of surface to represent the zeroes and ones or ON/OFF. See *A Byte of the Action*, *ECONOMIST*, Sept. 19, 1998, at 96.

to store<sup>10</sup> and use personal data has increased significantly, thus making the individual's personal information more susceptible to misuse.

For purposes of brevity, this Note is limited to a discussion of privacy as it pertains to personal data. Specifically, this Note focuses on the impact of the passage of the "European Parliament and Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," commonly referred to as the European Directive on Data Protection<sup>11</sup> (Directive), on the movement of personal data between the European Union and the United States.

The European Commission has elevated data privacy to a fundamental right.<sup>12</sup> The Directive is the means for ensuring that right by governing data privacy requirements. The Directive's breadth includes the movement of personal data between the Member States of the European Union, as well as the movement of such data to countries outside of the Europe-

---

10. There have been dramatic decreases in storage cost. For example, the amount of data that can be stored on a square inch of magnetic disk surface has increased by 60% per year since 1991. This has reduced the cost of storage media by a factor of 100 (the cost of storing one megabyte has been reduced from \$5.00 to \$0.05 over the same period). With respect to required space, this permits storage of roughly 340 copies of the 445 page Starr Report onto a cartridge which is smaller than a book of matches. *Id.*

11. Council Directive 95/46 of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Council Directive 95/46 1995 O.J. (L 281) 31 [hereinafter Directive]. The Directive was preceded by the Common Position (EC) No 1/95 with a view to adopting Directive 94/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (C 93) [hereinafter Common Position], and was adopted in its final state on October 24, 1995. *Id.*

12. See Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 15 (1998). Professor Simitis, speaking at the Annenberg Washington Program on Oct. 6, 1994 observed that:

"[t]he need for the Directive is based on the need to protect human rights within the Community . . . . This is why . . . we speak . . . of the necessity to respect the fundamental rights of citizens. Therefore, data protection may be a subject on which you can have different answers to the various problems, but it is not a subject you can bargain about."

*Id.* Professor Semitis, the former Data Protection Commissioner of the German State of Hesse and Chair of the Council of Europe's Data Protection Experts Committee, is one of the EU's most distinguished data protection experts. *Id.*

an Union, also known as "third countries."<sup>13</sup>

The Directive requires that transfers of personal data be permitted "only if . . . the third country in question ensures an adequate level of data protection."<sup>14</sup> The Directive's approach to cross-border data has in fact been likened to the erection of a "fence" around Europe.<sup>15</sup> Because the flow of personal data is an indispensable component of a global economy,<sup>16</sup> some safety valve was necessary, at least as a stop-gap measure, to provide an opening through this erected data "fence" in order to continue the orderly process of international trade. This safety valve has assumed the form of six exceptions to the general embargo of data to third countries.<sup>17</sup>

13. In a sense one could infer there is a suggestion that those countries that do not provide the level of protection required to comply with the Directive are "third world countries" with respect to data privacy. Indeed countries that do not comply are referred to as "data protection outlaw nations." As the current laws of privacy in the United States with respect to data protection are not on par with the Directive, this would appear to make the United States a "data protection outlaw nation." See Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 484 (1995). It is ironic that a nation that acknowledged the need for a "right to privacy" in 1890, see Warren & Brandeis, *supra* note 8, no longer finds itself in a leadership role in guaranteeing these rights, but instead has been relegated to an outcast status.

14. Directive, *supra* note 11, art. 25(1).

15. See Schwartz, *supra* note 13, at 484 n.94 (quoting from *A Commentary by the UK Data Protection Registrar*, in NINTH ANNUAL REPORT OF THE DATA PROTECTION REGISTRAR 66-75 (1993) ("If there is to be a Community with an acceptable and high level of individual data protection . . . it is to be expected that there will be a fence around the Community with some means of guarding it.")).

16. See REINHARD ELLGER, DER DATENSCHUTZ IM GRENZUEBERSCHREITENDEN DATENVERKEHR 108-29 (1990). See Schwartz, *supra* note 13, at 471 n.1. The most frequent transborder data transfers are:

- (1) personnel departments; (2) banks, insurance companies, credit card companies, and credit bureaus; (3) direct marketing; (4) airlines, travel agencies, and other businesses involved in the tourist industry; (5) companies that seek to deliver goods to or trade with international customers; (6) within the public sector: police, customs, tax departments, and public pension agencies.

*Id.* For a description of the rapid increase in data flows in the credit card business alone, see JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE 230-31 (1974), which discusses the tremendous growth of international data flows. For example Visa (then BankAmericard) grew from one million cardholders worldwide to 28.2 million cardholders within the first ten years of existence. *Id.*

17. See Directive, *supra* note 11, art. 26(1). The exceptions provided by Section 1 of the article are:

1. the data subject has given his consent unambiguously to the proposed transfer; or
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual

Some of these exceptions are not applicable to private enterprise; instead, they focus on the interests of the individual or public policy. However, all the exceptions which are applicable to business transactions fall within a contractual scope. Thus, the central purpose of this Note is to specifically address whether these contractual relations are an adequate means for ensuring data privacy and, if so, whether the contractual approach should be utilized.

Section II of this Note provides the reader with a fundamental perspective on differences between the United States and the European Union with respect to privacy law, and then summarizes some of the significant privacy protection goals of the Directive. Section III briefly discusses the potential implications of failure by the United States to ensure adequate protection of personal data. Section IV explains the contracts exception, which may be used to overcome shortcomings in U.S. law and examines its applications and shortcomings, suggesting that the contractual approach is better suited for large enterprises but problematic for businesses of smaller size. Section V provides some observations on why the United States is not prepared to adopt the Directive's approach, but concludes that greater data protection must be ensured in the United States because of advances in data processing technology and biotechnology.

## II. HISTORICAL PERSPECTIVE—A BRIEF REVIEW OF INDIVIDUAL PRIVACY IN THE UNITED STATES AND THE EUROPEAN UNION

The European Union's approach to data privacy differs

- 
- measures taken in response to the data subject's request; or
3. the transfer is necessary for the conclusion or for the performance of a contract concluded in the interest of the data subject between the controller and a third party; or
  4. the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
  5. the transfer is necessary in order to protect the vital interests of the data subject; or
  6. the transfer is made from a register which according to laws and regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

*Id.*

from that of the United States by taking an omnibus approach to individual rights and giving the state not only an active, but also pro-active preventive role.<sup>18</sup> The European emphasis is on the deterrence of harm and accomplishes this by instituting the necessary control mechanisms for oversight. In contrast, the United States uses a complex patchwork of laws (the Constitution, federal and state legislation, and state common law) to address the right to privacy, taking a reactive stance by legislating in narrow specific areas where problems have occurred.<sup>19</sup> The U.S. emphasis is on use of remedies for damage which has already taken place and prevents future harm by the threat of legal action. This pivotal difference is best explained by providing a general overview of the histories of privacy law in the United States and the countries of the European Union.

#### A. *Foundations of Privacy Law in the United States*

The United States originated as a group of colonies, many exercising a significant amount of self-government, that were formed into a federation of states.<sup>20</sup> As is well known, the underlying basis for this configuration was the colonists' fear of a strong central government.<sup>21</sup> As a result, the United States has a federal government founded upon a Constitution which established the balance of power between the states, their citizens and the federal government. The focus of the Constitution itself is the separation of power between the three branches of the federal government and the authority of the federal government in relation to the states.<sup>22</sup> A Bill of Rights was created later to address the bulk of citizens' rights.<sup>23</sup>

The rights guaranteed by the Bill of Rights, and later amendments to the Constitution which relate to the right to privacy, are the right to freedom of association, voting rights, protection from unreasonable search and seizure, and the right

---

18. See SCHWARTZ & REIDENBERG, *supra* note 8, at 5.

19. *Id.* at 5-9.

20. JOHN R. VILE, A COMPANION TO THE UNITED STATES CONSTITUTION AND ITS AMENDMENTS 1 (2d ed. 1997).

21. EDWARD F. COOKE, A DETAILED ANALYSIS OF THE CONSTITUTION 20 (6th ed. 1995). See also VILE, *supra* note 20, at 124.

22. See COOKE, *supra* note 21, at 18, 20.

23. *Id.* at 19.

to informational privacy, including avoiding disclosure of personal matters, and to independence in decision making.<sup>24</sup> Significantly, all of these rights protect an individual against the state, but not against the actions of other citizens. That is, the government may not infringe on the rights of citizens, but has no affirmative duty to prevent another citizen from doing so.<sup>25</sup>

Concomitantly, the rights of individuals against private parties are primarily found in state tort law.<sup>26</sup> By definition, because tort law varies from state to state such rights do not protect all U.S. citizens, but are reserved to the inhabitants of the states that recognize the cause of action.<sup>27</sup> Although privacy law is broadly defined by the Restatement (Second) of Torts, the Restatement is only secondary, not primary authority, and thus not binding on the courts of a state unless that state chooses to follow the guidance of the Restatement.<sup>28</sup> Privacy law in the Restatement encompasses: 1) an unreasonable physical intrusion upon the seclusion of another;<sup>29</sup> 2) the appropriation of another's name or likeness;<sup>30</sup> 3) unreasonable publicity given to another's private life;<sup>31</sup> and, 4) publicity that unreasonably places another in a false light before the public.<sup>32</sup>

---

24. See SCHWARTZ & REIDENBERG, *supra* note 8, at 44-90.

25. *Id.* at 32. An exception is the 13th Amendment prohibiting slavery, which protects the rights of former slaves against individuals, thus limiting private behavior. U.S. CONST. amend XIII. See SCHWARTZ & REIDENBERG, *supra* note 8, at 32 n.5. See also COOKE, *supra* note 21, at 180.

26. After the publication of *The Right to Privacy* by Samuel D. Warren and Lois D. Brandeis, *supra* note 8, another seventy years passed before Dean Prosser analyzed the various state forms of the "right to privacy" and categorized them into the four torts found in the *Restatement (Second) of Torts*. RESTATEMENT (SECOND) OF TORTS § 652A (1976). See also *infra* Section II.A.

27. See CHRISTINA L. KUNZ ET AL., THE PROCESS OF LEGAL RESEARCH 104-05, 112 (3d ed. 1992).

28. *Id.* at 7.

29. See RESTATEMENT (SECOND) OF TORTS § 652B (1976). Since this tort consists of an unreasonable intrusion into the seclusion of another, it at best applies to data collection with respect to data privacy. It requires an intrusion into another's private affairs that is "highly offensive to a reasonable person." *Id.*

30. *Id.* § 652C. This tort concerns itself with the commercial value inherent in a person's name or likeness, and thus is of limited value with respect to data privacy. Most states that recognize this tort require that the appropriation be for "commercial gain," such as advertising. *Id.*

31. *Id.* § 652D. This tort applies when there is a disclosure to a large audience of private information such that it would be "highly offensive to a reasonable person" and not be of "legitimate concern to the public." *Id.*

32. *Id.* § 652E. A publication to be actionable under this tort must be both false and highly offensive to the reasonable person. Thus, any information pub-



With the Great Depression and a shift to a national economy, the federal government began implementing increasingly broader legislation to stimulate the economy and provide benefits for those in need. Later, however, the legislation covered a multitude of areas, including those that are related to a person's right to privacy.<sup>33</sup> However, these forays into privacy law, which can best be described as "ad hoc," have been targeted at specific government agencies, economic sectors or industries, and often address only narrow and specific issues.<sup>34</sup> This has resulted in curiously inconsistent and uneven approaches to privacy protection.<sup>35</sup>

In an attempt to use a uniform approach to the protection of computer processed information, the Advisory Committee on Automated Data Systems, a subcommittee of the Health Education and Welfare Committee<sup>36</sup> issued a report addressing data protection in 1973.<sup>37</sup> That report, entitled, "Personal Data Systems: Records, Computers and the Rights of Citizens," listed five principles which were considered necessary to protect a person's privacy interest in information collected concerning him.<sup>38</sup> The response to the report was the passage of several statutes<sup>39</sup> which incorporated these principles. Howev-

---

lished which is true is not actionable and therefore offers no protection for the privacy of a person. *Id.*

33. See SCHWARTZ & REIDENBERG, *supra* note 8, at 7-8.

34. See CATE, *supra* note 2, at 80. See also SCHWARTZ & REIDENBERG, *supra* note 8, at 10.

35. See CATE, *supra* note 2, at 80-81.

36. The Department of Health, Education, and Welfare is today the Department of Health and Human Services. See DAVID H. FLAHERTY, *PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES* xxi (1989).

37. See Patricia Mell, *A Hitchhiker's Guide to Trans-border Data Exchanges Between EU Member States and the United States Under the European Union Directive on the Protection of Personal Information*, 9 PACE INT'L L. REV. 147, 159 (1997).

38. *Id.* n.70. The report annunciated five fundamental principles with regard to an individual's right to privacy: 1) the individual's right to determine what files exist about him; 2) knowledge how information by the individual will be used; 3) requirement that the individual consent to broader use of the information than originally contemplated by the record holder; 4) right of the individual to access the files and the opportunity by him to correct outdated or incorrect information; 5) files should receive adequate security and should be maintained correctly.

39. *Id.* n.71. Some of the statutes enacted, which incorporate these principles were: Privacy Act of 1974, 5 U.S.C. § 552a (1994); Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o) (1994); Privacy Protection Act of 1980, 42 U.S.C. § 2000(aa)-(aa)(12) (1994); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1994).

er, because each of these statutes was limited to a specific area or sector, the resulting protection for the individual was neither comprehensive nor consistent. This phenomenon is most evident when one juxtaposes the limited privacy regarding one's medical condition and treatment with the considerable protection given to information concerning an individual's video rentals.<sup>40</sup>

Another example of the inconsistent privacy protection phenomenon can be seen in the federal Privacy Act of 1974<sup>41</sup> (Privacy Act). The Privacy Act is one of the earliest laws governing data privacy and indeed is quite comprehensive, even though it only applies to governmental agencies. The Privacy Act requires government agencies to (1) store only necessary and relevant information;<sup>42</sup> (2) collect that information from the data subject itself to the extent this is possible;<sup>43</sup> (3) maintain records with accuracy and completeness;<sup>44</sup> and (4) protect the security of records through establishment of administrative and technical safeguards.<sup>45</sup> While these protections are significant and are mirrored by those of the European Directive, the effectiveness of the Privacy Act is undermined by its many exclusions. For example, the Privacy Act specifically states that it does not apply to any information for which disclosure is required under the Freedom of Information Act.<sup>46</sup>

In addition to this limitation, the Privacy Act has twelve exemptions that allow information to be disclosed to other government agencies, including Congress.<sup>47</sup> The broadest ex-

---

40. See Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy, and Health Care Reform*, 23 HASTINGS CENTER REP. 13, 13 (Nov.-Dec. 1993). Sheri Alpert is a government policy analyst who summarized the situation as follows: "video rental records are afforded more federal protection than are medical records." *Id.* See also SCHWARTZ & REIDENBERG, *supra* note 8, at 7-11. The Video Privacy Protection Act of 1988, also known as the "Bork Bill" came into existence after a public uproar following the publication of a list of video titles rented by then federal appellate judge and nominee for the United States Supreme Court, Robert Bork. See also Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710-2711 (1994)).

41. 5 U.S.C. § 552a (1994).

42. *Id.* § 552a(e)(1).

43. *Id.* § 552a(e)(2).

44. *Id.* § 552a(e)(5, 6).

45. *Id.* § 552a(e)(10).

46. *Id.* § 552a(b)(2). Note that the Freedom of Information Act permits persons access to all agency records, subject to nine exemptions. *Id.* § 552(b).

47. 5 U.S.C. § 552a(b)(1)-(12).

emption of the Privacy Act is for any data requested by another government agency for "routine use."<sup>48</sup> This exemption has been used by government agencies to such an extent that it has prompted Professors Schwartz and Reidenberg to observe that the "routine use" exemption has been employed to justify almost "any use" of data.<sup>49</sup>

In addition to a large number of federal statutes, state law also protects the citizens of individual states through constitutional and statutory laws.<sup>50</sup> A number of state constitutions, unlike the federal Constitution, expressly protect privacy.<sup>51</sup> However, like the federal Constitution, such protections are generally limited to the right of the citizen against the government and do not regulate relations between citizens.<sup>52</sup>

With regard to the statutory provisions of the individual states, they tend to fall into three categories: (1) some states have codified the common law torts discussed previously, thereby creating a general right to privacy; (2) other states have limited such statutes to one or more of the common law privacy torts; and (3) yet other states have promulgated industry-specific privacy legislation, which like their federal counterparts take a narrow sectoral approach.<sup>53</sup>

In the final analysis, the approach to privacy in the United States has been one of restraint. The result is minimal restrictions that ensure a free flow of information. This path is philosophically consistent with the strong tradition of a laissez-faire state—which calls for minimal interference of government upon the private sector, and thus allows for the free flow of

---

48. *Id.* § 552a(b)(3).

49. See SCHWARTZ & REIDENBERG, *supra* note 8, at 98.

50. *Id.* at 9.

51. See ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy").

52. The California Constitution is a rare exception that applies the right of privacy equally to private parties and the government. See generally *Hill v. N.C.A.A.*, 865 P.2d 633 (Cal. 1994).

53. See Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 227-229 (1992).

ideas as exemplified by both freedom of speech and protection of the press.<sup>54</sup>

### *B. Foundations of Privacy Law in the European Union*

Although it was the United States that originated the right to privacy, the first data privacy legislation was passed in Europe, in the German state of Hesse in 1970.<sup>55</sup> Today, however, Austria, Belgium, Denmark, France, Germany, Ireland, Luxembourg, the Netherlands, Spain, Sweden, and the United Kingdom all have broad data protection or privacy statutes.<sup>56</sup>

The interest in personal privacy in European countries has its roots in twentieth century European history. It has been suggested that to some extent the hidden agenda behind the European data protection laws is Europe's experience in World War II, and the desire to avoid a recurrence of the type of population control exercised by the Nazis and the Gestapo.<sup>57</sup>

Modern day protection of personal information privacy through the Directive finds its source in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (Human Rights Convention),<sup>58</sup> which guarantees the right of privacy involving "private and family life . . . home . . . and correspondence."<sup>59</sup> Although the threat to personal privacy was recognized by the Human Rights Convention in 1950, the concern for the protection of privacy was heightened by the expansion of computer use and the associated shift from an industrial economy to an information economy.<sup>60</sup>

To ensure that the right to privacy would not be infringed

---

54. See SCHWARTZ & REIDENBERG, *supra* note 8, at 6-7.

55. See Cate, *supra* note 12, at 5.

56. *Id.*

57. See FLAHERTY, *supra* note 36, at 373-74. See also Grundgesetz (federal constitution) [GG] arts. 1, 10, 13 (F.R.G.), showing that the right to privacy was included in the German Constitution after WWII.

58. Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter Human Rights Convention]. The provisions of the Convention are applicable by their own force and effect as they supersede European National Laws. See generally M. CHERIF BASSIOUNI, INTERNATIONAL EXTRADITION 501 (2d ed. 1987). See also Mell, *supra* note 37, at 158.

59. See Human Rights Convention, *supra* note 58, art. 8(1).

60. See generally DANIEL BELL, THE COMING OF POST-INDUSTRIAL SOCIETY (1973).

upon by the advent of technology, the Council of Europe (hereafter Council) began "to study potential courses for data protection legislation."<sup>61</sup> This study resulted in a resolution passed by the Council in 1974 which addressed the storage of personal data.<sup>62</sup> The guidelines of the resolution subsequently became incorporated in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Personal Data Convention) in 1981.<sup>63</sup> It is this Convention that formed the basis for what was to become the Directive.<sup>64</sup>

The Personal Data Convention addresses data quality by requiring that data be: (1) fairly and legitimately obtained and processed; (2) used and stored for legal purposes; (3) adequate, relevant and not excessive with respect to the purpose for which it is stored; (4) up to date and accurate; and (5) maintained no longer than is necessary to achieve its purpose.<sup>65</sup>

61. Peter Mei, *The EC Proposed Data Protection Law*, 25 LAW & POL'Y INT'L BUS. 305, 307 (1993). See also Michael Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 71, 75 (1996).

62. See *On The Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Public Sector*, Council of Europe Res. (74) 29 (1975). The resolution's requirements are that: 1) the public be informed about electronic data banks; 2) information stored be obtained by lawful and fair means, be accurate and up to date, and be appropriate and relevant with respect to the purpose for which it was stored; 3) where information is private or could lead to discrimination, such use of information must be regulated and ensured by competent authorities; 4) time limits be placed on the length of time for use of such information; 5) individuals should know what data is stored concerning them; 6) precautions against abuse or misuse of information are to be applied by administrative and technical means; 7) access to the data should only be available to those with a legitimate purpose; and 8) information for statistical use is to be released in a way that prevents linkage to the individuals whose data was incorporated in the results. *Id.* See also Cole, *supra* note 7, at 898 (listing principles of a progenitor resolution addressing the private sector as 1) a person's private information, or information which may result in discrimination should not be disseminated; 2) only relevant information is to be stored; 3) rules regarding collection, storage and dissemination of data are to be implemented; 4) individuals should know what data is stored concerning them, where it is stored, and the purpose of the stored data; 5) individuals should have the right to correct or delete incorrect data concerning them; 6) access to the data should only be available to those with a legitimate purpose).

63. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, Europ. T.S. No. 108 (entered into force on Oct. 1, 1985) [hereinafter Personal Data Convention]. See also Ulrich U. Wuermeling, *Harmonisation of European Union Privacy Law*, 14 J. COMPUTER & INFO. L. 411, 415-17 (1996).

64. See Wuermeling, *supra* note 63, at 416-23.

65. See Personal Data Convention, *supra* note 63, art. 5.

Article 8 of the Personal Data Convention also gives rights to individuals concerning their data by allowing them to make inquiries into any data gathering organization which has files regarding them; receive a copy of the data in readable form; correct or delete false or otherwise improperly kept data; and if the individual is denied access to the data or a copy of it, he may request the data be deleted.<sup>66</sup> As the Personal Data Convention was not self-executing<sup>67</sup> and lacked definitions, individual European countries implemented their own legislation with requisite definitive terms.<sup>68</sup> Because the various European countries were at different stages of addressing this issue, for some countries this meant implementing legislation,<sup>69</sup> while other countries already had appropriate legislation at the time of the passage of the Personal Data Convention.<sup>70</sup> Unfortunately, implementation of privacy legislation by European countries at different times, and their use of diverse approaches, contributed to a lack of harmony between their laws thereby resulting in provisions restricting the flow of data between countries.<sup>71</sup>

Although the European Commission (Commission) recommended to its Member states that they ratify the Personal Data Convention,<sup>72</sup> it still had not been ratified in 1990 by five

---

66. *Id.* art. 8.

67. See SPIROS SIMITIS ET AL., KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ §1, at 122 (1992). Non-self-executing means that each Member state is required to pass enabling legislation for the Data Privacy Convention to become effective in that state. See also Wuermeling, *supra* note 63, at 418.

68. See Mei, *supra* note 61, at 308.

69. *Id.*

70. Sweden was the first European country to pass a national data privacy law in 1973. See Cole, *supra* note 7, at 902-03. Although the German state of Hesse passed its first data protection law in 1970, it was merely state law and applicable only to the public sector. *Id.* at 903. The German federal government passed its national law on the Protection of Personal Data against Misuse in Data Processing in 1977, which was patterned after the 1970 Hesse state law. See Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung, 1977 (BGBl. I S.201) (F.R.G.). The seriousness of the German authorities with respect to these rights is demonstrated by the applicable fines and/or punishment one is subject to for violating them. For example, where one obtains, modifies, or transmits protected personal information without a legal right to do so, one is subject to fines or incarceration not to exceed one year, or, where such acts are committed for one's own enrichment, or the enrichment of another, or the purpose of the act is to damage another, incarceration of up to two years is possible. *Id.* § 41 (translation from German is the author's).

71. See Mei, *supra* note 61, at 308.

72. See Wuermeling, *supra* note 63, at 419.

of the Member states of the European Community.<sup>73</sup> As a result, the Commission changed its approach by no longer pursuing ratification of the Personal Data Convention.<sup>74</sup> Instead, the Commission published its First Proposal for a Data Protection Directive,<sup>75</sup> which, after review and comments by the appropriate political bodies, was followed by the Commission's Second Proposal two years later.<sup>76</sup>

In 1995, the Commission introduced the Directive in its current form<sup>77</sup> with the goal of securing an equivalent level of personal data protection among the Member states.<sup>78</sup> With this goal, the Directive aspired for the elimination of obstacles to the free movement of data across borders which could occur due to inconsistent levels of data protection between Member states,<sup>79</sup> as well as the protection of fundamental rights and freedoms in Europe.<sup>80</sup> It is this commitment by the European Union which shows that, although economic incentives were at play, other major driving forces were social and political matters for the European Union.<sup>81</sup> This belief was well expressed by the French Data Protection Commissioner Jaques Fauvet, when he asked, "Do we want a Europe of merchants or one of human rights?"<sup>82</sup>

In recognition that the new information society required the unimpeded flow of data, the Directive, per article 1(2), sought to ensure the free flow of data streams within the Euro-

---

73. *Id.* at 420. The five countries which failed to ratify the convention were Belgium, Greece, Italy, Portugal, and Spain. *Id.*

74. *Id.*

75. Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277) 3 [hereinafter First Proposal]. The First Proposal was based on three main data protection ideas which had already been seen in the Data Protection Convention: (1) that limitations be placed on processing of data; (2) that there be transparency to the data subject; (3) that there be safeguards with respect to data integrity and security. *See Id.* arts. 6, 9, 18.

76. Amended Commission Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1992 O.J. (C 311) 30 [hereinafter Second Proposal].

77. *See generally* Directive, *supra* note 11.

78. *Id.*

79. Common Position, *supra* note 11, at 2.

80. *Id.* at 3.

81. *See* STEPHEN WEATHERILL & PAUL BEAUMONT, EC LAW 23 (1993). *See also* Schwartz, *supra* note 13, at 480.

82. Schwartz, *supra* note 13, at 480 n.61 (citing Commission nationale de l'informatique et des libertes, 14e rapport d'activite 75 (1993)).

pean Union rather than just the general protection of personal data.<sup>83</sup> Article 1(2) states "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."<sup>84</sup> This additional requirement is reflected in the change of the Directive's title between the First and the Second proposal by the addition of the words "and on the free movement of data."<sup>85</sup>

In order to achieve the free flow of data and the protection of personal data, the Directive has as its goal an equivalent level of protection of personal data among all its Member states.<sup>86</sup> However, in terms of data sent to third countries outside the European Union, the Directive changes its approach by requiring an "adequate" level of protection, as opposed to an "equivalent" level of protection.<sup>87</sup>

Yet another change in the Directive as announced in the Second Proposal is that, in general, the Directive no longer distinguishes between the public and private sectors, and thus fosters the protection of individuals from both spheres.<sup>88</sup> It is precisely this protection by the Directive from both the private and public sectors that marks one of the major differences between the protection afforded Europeans and American citizens—thus a reason that there is neither equivalence nor ade-

---

83. See Wuermeling, *supra* note 63, at 426-27.

84. See Directive, *supra* note 11, art. 1(2).

85. *Id.* at 31. See also Wuermeling, *supra* note 63, at 427.

86. Because of the different means of achieving protection of personal data among the various member states, the best that can be achieved by the Directive is equivalent, not equal protection. However, as long as the Directive sets a floor that is acceptable to all the Member states, the fact that some of the states will have higher levels of data protection within their own borders should not be an obstacle.

87. Directive, *supra* note 11, art. 25(4) (Directive requirement of protection of individuals in the European Community).

88. See Wuermeling, *supra* note 63, at 428. However, the Directive's human rights provision draws an important distinction between the public and private sectors: human rights are concerned with the interaction between the public authorities and its citizens, while the private sector deals with the interaction between individuals in a non-public sphere. See Directive, *supra* note 11, preamble, para. 5.



quacy of protection offered under U.S. law, as discussed below.<sup>89</sup>

### C. *The Primary Data Privacy Protection Goals of the Directive*

An in-depth discussion of the Directive is beyond the scope of this Note. However, a background of the approach to personal data protection of the Directive is required to appreciate the disparity between the level of protection afforded under the Directive and that provided under U.S. law, and to understand how the gap may be filled with a contractual approach. To achieve this understanding, a review of selected articles is in order. The relevant articles are:

Article 1. This article defines the objectives of the Directive as protecting the fundamental rights and freedoms of persons with respect to the processing of personal data<sup>90</sup> and ensuring the free flow of data between the Member states.<sup>91</sup>

Article 2. This article provides definitions of the following terms and phrases: "personal data,"<sup>92</sup> "processing of personal data,"<sup>93</sup> "personal data filing system,"<sup>94</sup> "controller,"<sup>95</sup> "proces-

89. See generally *supra* Section II.A.

90. See Directive, *supra* note 11, art. 1(1).

91. *Id.* art. 1(2).

92. *Id.* art. 2(a).

'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

*Id.*

93. *Id.* art. 2(b).

'[P]rocessing of personal data' ('processing') 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.

*Id.*

94. *Id.* art. 2(c). "[P]ersonal data filing system' ('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." *Id.*

95. See *Id.* art. 2(d).

'[C]ontroller' shall mean the natural or legal person, public authority, agency or any other body which determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations,

sor,<sup>96</sup> "third party,"<sup>97</sup> and "recipient."<sup>98</sup>

Article 6. This article establishes data quality principles and requires the Member states to ensure that personal data is processed fairly and lawfully;<sup>99</sup> is collected for specified purposes and not further processed in ways incompatible with the original purpose;<sup>100</sup> is adequate, relevant, and not excessive for the purpose for which it was collected;<sup>101</sup> is accurate and kept up to date; and reasonable steps are taken to correct or erase inaccurate data.<sup>102</sup> It also requires that data is kept in a form which permits identification of the data subject for the shortest time, and that data kept for longer periods, which will be used for historical, statistical, or scientific use, have appropriate safeguards applied to them.<sup>103</sup>

Article 8. This article deals with special categories of data processing and prohibits the processing of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning health or sex life."<sup>104</sup> This prohibition is narrowly circumscribed by exceptions<sup>105</sup> dealing with: (a) party's consent;<sup>106</sup> (b) authorized employment law purposes;<sup>107</sup> (c) data processing vital to the data subject's interest and subject's

---

the controller or the specific criteria for his nomination may be designated by a national or Community law.

*Id.*

96. Directive, *supra* note 11, art. 2(e). "[P]rocessor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." *Id.*

97. *Id.* art. 2(f). "[T]hird party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the person who, under the direct authority of the controller or processor, are authorized to process the data." *Id.*

98. *Id.* art. 2(g). "[R]ecipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients." *Id.*

99. *Id.* art. 6(1)(a).

100. *Id.* art. 6(1)(b).

101. *Id.* art. 6(1)(c).

102. Directive, *supra* note 11, art. 6(1)(d).

103. *Id.* art. 6(1)(e).

104. *Id.* art. 8(1).

105. *Id.* art. 8(2).

106. *Id.* art. 8(2)(a).

107. *Id.* art. 8(2)(b).

physical or legal inability of giving consent;<sup>108</sup> (d) processing conducted for legitimate purposes and with appropriate guarantees by a designated organization relating only to members of that organization, subject to third party disclosure only with the data subject's consent;<sup>109</sup> and (e) data which has manifestly been made public by the data subject, or data necessary in pursuit of a legal action.<sup>110</sup>

Article 10. This article deals with the rights of the data subject where the data has been directly collected from the subject itself and provides that the subject be (a) informed of the data processor's identity,<sup>111</sup> (b) told of the purposes of the data processing;<sup>112</sup> and, (c) provided with the identity of recipients or categories of recipients of the data, whether the responses are obligatory or not, and the consequences of failing to reply, the existence of a right to access and rectify data collected, and the guarantee of fair data processing.<sup>113</sup>

Article 11. This article deals with the rights of the data subject where the data has not been directly obtained from the subject itself. It provides that the subject be supplied with the following information no later than the time at which the data is to be disclosed: (a) the data processor's identity;<sup>114</sup> (b) the purposes of the data processing;<sup>115</sup> and (c) the categories of data concerned. It also requires that the subject be notified of the identity or categories of recipients. Finally, it requires notification of the right to access and rectify data collected, and the guarantee of fair data processing.<sup>116</sup>

Article 12. This article discusses the data subject's right to access the data collected about him. It requires that every data subject have the right to obtain information, without excessive delay or expense, whether data relating to the subject has been

---

108. Directive, *supra* note 11, art. 8(2)(c).

109. *Id.* art. 8(2)(d). The type of organization is described as "a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim," and requires "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." *Id.*

110. *Id.* art. 8(2)(e).

111. *Id.* art. 10(a).

112. *Id.* art. 10(b).

113. *Id.* art. 10(c).

114. Directive, *supra* note 11, art. 11(a).

115. *Id.* art. 11(b).

116. *Id.* art. 11(c).

processed, the purpose of the processing, the categories of data concerned and the recipients of the data, and if any automated decision-making was made which might produce a legal effect for the data subject.<sup>117</sup> As appropriate, the rectification, erasure or blocking of data which does not comply with the Directive due to incompleteness or inaccuracies, is called for.<sup>118</sup> Also, subjects, as well as third parties to whom the data has been disclosed, must be notified of corrections unless it is impossible or results in a disproportionate effort.<sup>119</sup>

Article 17. This article addresses the security of data processing and requires that appropriate technical and organizational measures exist to protect the integrity of personal data exist.<sup>120</sup> Where processing is carried out by another party, that party must also comply with such security measures.<sup>121</sup>

Article 22. This article provides every person the right "to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question."<sup>122</sup>

Article 23. This article provides that "any person who has suffered damage as a result of an unlawful processing operation . . . is entitled to receive compensation from the controller for the damage suffered."<sup>123</sup> However, "[t]he controller may be exempted from his liability . . . if he proves that he is not responsible for the event giving rise to the damage."<sup>124</sup>

In summary, the Directive provides for comprehensive protection of personal data by ensuring four essential elements of fair information practice: "(1) the establishment of obligations and responsibilities for personal information; (2) the maintenance of transparent processing of personal information; (3) the creation of special protection of sensitive data; and (4) the establishment of enforcement rights and effective oversight

---

117. *Id.* art. 12(1). The type of legal effect in question here is one which "significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." *Id.* art. 15(1).

118. *Id.* art. 12(2).

119. *Id.* art. 12(3).

120. Directive, *supra* note 11, art. 17(1).

121. *Id.* art. 17(2).

122. *Id.* art. 22.

123. *Id.* art. 23(1).

124. *Id.* art. 23(2).

of the treatment of personal information."<sup>125</sup> Since these broad protections pertain to both the public and private sectors, they provide significantly more protection than those offered to citizens of the United States, where the focus of protection is only on public institutions.<sup>126</sup> As a result, the protection of personal data in the United States falls short of those announced by the European Directive.<sup>127</sup>

---

125. SCHWARTZ & REIDENBERG, *supra* note 8, at 13. It is interesting to note that these four elements of the Directive, while more comprehensive, address essentially the same concerns as the five principles listed in the Advisory Committee on Automated Data Systems 1973 report on "Personal Data Systems: Records, Computers and the Rights of Citizens." See Mell, *supra* note 37, at 159 (listing the five fundamental principles of privacy announced by the 1973 report by the Advisory Committee on Automated Data Systems).

126. See generally *supra* Section II.A.

127. See generally SCHWARTZ & REIDENBERG, *supra* note 8. It is important to note that because the adequacy of U.S. data privacy law varies significantly from sector to sector, it is inappropriate to attempt to answer the question of U.S. data protection as a totality. Rather, there is a need to acknowledge that the protection personal data receives in the United States may in some sectors be adequate although it does not meet the spirit of the Directive, while in other sectors will likely be viewed as extremely problematic by the European Commission. It is beyond the scope of this Note to provide such an analysis, but the assertion that data privacy is inadequate to ensure the protection provided by the Directive is easily verifiable by other scholarly works which have addressed this question. For example, Professor Fred H. Cate stated that with respect to telecommunication privacy "[e]ven in this highly regulated sector of the United States economy, United States law provides nowhere near the protection for personal data as is required by the data protection Directive . . . . This . . . raises serious questions about whether any other industry sector in the United States will be able to satisfy . . . the data protection Directive's adequacy requirement." See Cate, *supra* note 12, at 47. The seminal text in this area is *Data Privacy Law* by Professors Reidenberg and Schwartz which was written for the European Commission as a study of U.S. data protection law. This work provides a comprehensive analysis of U.S. data privacy law and employs sectoral analysis that strongly suggests that U.S. privacy law in general fails to provide the level of protection required by the Directive, and certainly fails to do so in specific sectors. See generally, SCHWARTZ & REIDENBERG, *supra* note 8. This sense of inadequacy of U.S. privacy protection is best expressed in the foreword to *Data Privacy Law* by the renowned European privacy law scholar, Professor Spiros Simitis, Professor of Law, Johann Wolfgang Goethe University, Frankfurt am Main, Germany, when he says that a reader of *Data Privacy Law* may be left:

with a distinct feeling of disappointment regarding the state of American data protection. Whoever has observed the processing practices, witnessed the intensive debates on the necessity of regulatory mechanisms and read the numerous both original and conclusive legislative proposals, will certainly expect more than the few islands of thorough regulation in the United States. But the study shows also that there are realistic chances for a quick development of comprehensive regulatory mechanisms fulfilling on a broad basis the demands of the "adequacy" principle.

### III. THE FAILURE OF UNITED STATES' PRIVACY LAW TO PROVIDE ADEQUATE PROTECTION AND ITS IMPLICATION ON DATA TRANSFER BETWEEN THE UNITED STATES AND THE EUROPEAN UNION

The failure of the United States' privacy law to provide a level of protection for personal data adequate to meet the goals of the Directive has serious implications for the future relationship between the European Union and the United States. This is necessarily so since the Directive has elevated the right to privacy for Europeans to the level of a fundamental right.<sup>128</sup> This right is not protected when data of European citizens is processed in the United States. To ensure that there are no privacy abuses, the Directive provides that trans-border data flow to a non-complying country may be prohibited by the individual Members of the European Union.<sup>129</sup> However, in an age where data flows of personal and business information are increasingly global, a blockage of data streams is likely to have serious political and economic consequences.

The Directive, contrary to most domestic laws in Europe which require an "equivalency standard" with respect to transfers between Member states,<sup>130</sup> requires that an "adequate level of protection" exist when data is transferred to third countries.<sup>131</sup> The requirement by most European nations that countries to whom they transfer personal data provide a level of protection "equivalent" to that provided in the country of origin is not to be confused with "equal" protection. This is because the approach and language of the laws of the various European countries differ.<sup>132</sup> The variety is understandable when considering that the Council's Personal Data Convention permitted a country's national laws to vary, and thus to exceed the basic protections of the Personal Data Convention.<sup>133</sup> Be-

---

*Id.* at x. For a discussion of the adequacy principle see *supra* Section II.B.

128. See Directive, *supra* note 11, art. 1(1). See also *supra* Section II.A.

129. See Directive, *supra* note 11, art. 25(4). The Article states that "[w]here . . . a third country does not ensure an adequate level of protection . . . Member States shall take the measures necessary to prevent the transfer of data . . . to the third country . . . ." *Id.*

130. The Directive explains that "the level of protection of the rights and freedoms of individuals with regard to the processing of . . . data must be equivalent in all Member States." Common Position, *supra* note 11, at 2.

131. See Schwartz, *supra* note 13, at 473.

132. *Id.* at 473-477.

133. Personal Data Convention, *supra* note 63, art. 4(1) (stating "[e]ach Party

cause some countries have higher levels of protection than that set by the Personal Data Convention, the citizens of such countries enjoy greater protection within their national borders than in the rest of the European Union.

The Directive's approach of "adequacy" as opposed to "equivalence" creates a lower tier of data protection for data flowing to third countries outside the European Union. The Directive's approach to determining "adequacy" is explained by Article 25(2):

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.<sup>134</sup>

Determinations concerning the adequacy of data protection in a third country will be made by the individual Member States themselves in accordance with Article 25(1).<sup>135</sup> Unfortunately, it is not at all clear what "adequacy" means in tangible terms for a country like the United States which has no system of oversight or registration, no independent data protection officials, and grants no legal rights to its citizens regarding access, opposition, or correction of data in most sectors of private endeavor.<sup>136</sup>

Because the enforcement of the "adequacy" of data protection must be ensured by the Member States, a European Un-

---

shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.")

134. Directive, *supra* note 11, art. 25(2).

135. *Id.* art. 25(1). Section One of the Article provides:

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.

*Id.*

136. See Cate, *supra* note 12, at 43-44.

ion Working Party was asked to clarify the operation of articles 25 and 26 of the Directive.<sup>137</sup> This group, on June 26, 1997, released a document which addressed both procedural and substantive components of "adequacy."<sup>138</sup> While this "white paper" offered insights into the Directive's adequacy requirements and suggested approaches for making adequacy determinations, it failed to narrow the Directive's requirements.<sup>139</sup>

At the same time, the "adequacy" approach has also sparked criticism from European experts who find it undesirable that data protection be lower in third countries than within the European Union. This is especially so since individuals within Europe are less likely to know what is happening to their data in foreign countries.<sup>140</sup>

Moreover, it is not clear whether the Directive's requirements set out a minimum (floor) or a maximum standard (ceiling). Because one purpose of the European Union was to facilitate free flow of goods, capital, and persons, this goal is best facilitated by having the European-wide law be the ceiling for what a Member State can require of another Member State. This would create no blockages of such free movement. On the other hand, if the Directive sets the floor, it will permit the

---

137. *Id.* at 44.

138. *Id.*

139. *Id.* at 46. Professor Cate stated that:

[S]ince the working party's interpretation of the Directive in no way narrows the Directive's requirements, it comes as no surprise that United States law fails to meet either the substantive or procedural data protection requirements identified by the working party. In fact, the working party's . . . [interpretation tends to] . . . highlight, rather than ameliorate, the differences between United States and European law.

*Id.* Because this analysis focused on telecommunication law, one of the most highly regulated sectors in the United States, it is implicit that U.S. law in general would not meet the Directive's requirements. This is especially so in areas of sensitive data such as medical records. *See also* Patrick J. Murray, Comment, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 *FORDHAM INT'L L.J.* 932, 991-994, 1016-1017 (1998) (maintaining that U.S. data protection in many areas of the private sector, such as health care and direct marketing, is inadequate).

140. *See* PETER DIPPOLDSMANN, *KRITISCHE JUSTIZ* 369, 377 (1994). Dippoldsmann points out that it is inconsistent to require a lower level of protection for data being sent to countries outside the European Union than within the EU because such transfers are riskier, less transparent and outside the jurisdiction of Member states and, therefore, should require higher, not lower, data protection requirements. He further suggests that the rationale for this "selective privacy protection" is based on the interest in the free flow of data. *Id.* *See also* Schwartz, *supra* note 13, at 485.



enforcement of higher local standards. This is implied by the language in Article 25(1) that "transfer[s] to a third country . . . may take place only if . . . [in] compliance with the national provisions adopted pursuant to . . . this Directive."<sup>141</sup> And according to the interpretation of one European expert, these international transfers of personal information will be compliant only when they also meet the higher protection standards found in the domestic law of the relevant Member State.<sup>142</sup> If the Directive were indeed interpreted to set a floor, than this would strongly suggest that U.S. legislation would have to adopt the highest standard among the European Member States to ensure ready access to the entire European Union.

While the free flow of information weighs strongly in favor of interpreting the Directive as setting a ceiling, it stands to reason that this approach is not desirable, perhaps even unacceptable to Member States that have previously been leaders in data protection, requiring them to relinquish rights they have already ensured their citizens through local legislation—in many cases legislation enacted prior to the establishment of the Directive. France and Germany, for example, have placed pressure on the European Union to interpret the requirements as a floor, expressing concern that interpreting the Directive as a ceiling would significantly, if not totally, curtail improvements in data privacy law in Europe.<sup>143</sup>

The seriousness of the Directive is emphasized in Section 3 of Article XXV which requires that the Member States and the European Commission inform each other of cases where a third country fails to provide adequate protection,<sup>144</sup> suggesting that lists of countries who have violated the Directive may be kept, and that data embargoes against specific countries will be implemented. This inference is supported by the language that the Commission "shall enter into negotiations with a view to remedying the situation."<sup>145</sup>

---

141. Directive, *supra* note 11, art. 25(1). See also Schwartz, *supra* note 13, at 487.

142. See Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 464-65 (1995). See also Schwartz, *supra* note 13, at 487.

143. See Schwartz, *supra* note 13, at 487.

144. Directive, *supra* note 11, art. 25(3).

145. *Id.* art. 25(5).

The Directive does provide limited exceptions to Article 25 in Article 26 which permit the transfer of data to non-compliant third countries.<sup>146</sup> The topic of this Note is the exception which concerns the execution of contracts to ensure adequate data protection of data transferred between data importers and data exporters.<sup>147</sup>

#### IV. THE CONTRACT EXCEPTION

The Directive's exception to the requirement of data protection adequacy applies when the parties involved in the data transfer have entered into a private contract. While this exception, in theory, provides a safety valve for private enterprise in cases where national laws are inadequate to ensure adequate data protection, it may be problematic in practice. Not only has this approach been criticized by European experts, but it also raises questions of practicality.

The contract exception to the adequacy requirement provides:

Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such guarantees may in particular result from appropriate contractual clauses.<sup>148</sup>

The purpose of the contract between the parties is to fill the gap between the Directive and the laws of the third country by having the European data exporter enter into a contract with the third country data importer to ensure "sufficient guarantees with respect to the protection of the privacy . . . rights . . . of individuals."<sup>149</sup> Given that it is unlikely adequate legislation in the United States will be forthcoming to reach an "adequate" level of protection, the contractual solu-

---

146. *Id.* arts. 26(1)-(2).

147. *Id.* art. 26(2).

148. *Id.*

149. *Id.*

tion seems to be the only safety valve to guarantee European citizens the requisite level of protection.

However, just as the disparity between "adequate" and "equivalent" levels of protection had critics among the Union's Member States, so does the contractual approach. Europeans have traditionally had more of their lives subject to legislation, such as health care and retirement pensions, so they are more likely to see the solutions to social problems in the hands of government rather than in the private sector. Thus, Europeans are naturally skeptical about using a contractual approach in lieu of legislation to ensure one of their fundamental rights.<sup>150</sup> A brief review of the use of contracts shows that while the contractual solution has merit, it also has some significant limitations.

#### A. *An Analysis of the Contractual Approach.*

To be effective, data privacy requires an enforcement mechanism. In Europe, this mechanism takes the form of registration or oversight by state officials and employees in private institutions. Any failure to comply with the national law implementing the requirements of the Directive is subject to injunctions and fines, and in some cases the potential for criminal liability exists. Because of the existence of public institutions and public or private individuals tasked specifically with ensuring compliance with the Directive, a person who suspects his rights have been violated has ready access to a remedy.

In comparison, the contractual approach requires a suit charging breach of contract for enforcement. Because of the high cost of litigation, this will likely lead to under-enforcement of privacy rights, if not minimal enforcement of those rights. In addition, the cost of creating a contract may be problematic for small institutions, especially when they have to determine what additional protections are required to reach the requisite level of protection.

This analysis is likely to be complex in a case involving a contract in the United States where protection varies from sector to sector, state to state, and is subject to different interpretations by different courts. In addition, a European citizen's lack of knowledge of what uses are made of his data in a dis-

---

150. See Schwartz, *supra* note 13, at 491.

tant third country with a different language, culture, and legal system further compounds the complexity of the situation.

A brief examination of two situations where contracts have been used to ensure personal data protection is instructive in that it highlights both positive aspects and limitations of what can be achieved with this approach. The first case involves an Italian automotive firm, Fiat, and its French subsidiary Fiat-France, while the second case involves the German Railway (Deutsche Bahn AG) and Citibank, an American financial institution.

In the case involving Fiat and its French subsidiary Fiat-France, the CNIL,<sup>151</sup> (French Privacy Commission), exercised its data embargo power to negotiate a contract between these two entities.<sup>152</sup> At issue was a transfer of data concerning the Fiat-France employees to the main firm in Italy.<sup>153</sup> Because Italy at the time of the transfer had not yet legislated its national data protection law, the French employees were not guaranteed that their data would be protected in Italy as it was under French national law.<sup>154</sup> In order that the data could be transferred from France to Italy, the main branch of Fiat was required to enter into a contract with its French subsidiary, obliging it to give the data the same protection it would have received under French law.<sup>155</sup>

While this approach seems perfectly adequate on the surface, it must be recognized that once the data is transferred to Italy, the French Privacy Commission lacks jurisdiction to enforce the contract in Italy.<sup>156</sup> As a result, compliance with the contract, and thus the assurance of data protection, depends on either Fiat-Italy taking adequate steps to comply with it voluntarily, or on Fiat-France auditing Fiat-Italy for compliance. Both scenarios suggest difficulties. Even if Fiat-Italy in good faith intends to honor its contract, if Italian law does not require an equivalent level of data protection, it is unlikely that Fiat in Italy will have staff who are trained to

---

151. CNIL is the abbreviation for the commission nationale de l'informatique et des libertés. See Schwartz, *supra* note 13, at 474 n.13.

152. *Id.* at 491-492.

153. *Id.* at 492.

154. *Id.*

155. *Id.*

156. *Id.*

ensure compliance. If, on the other hand, Fiat-France audits its parent in Italy and finds transgressions, it is difficult to imagine that it would report its parent company to the French authorities once the data has been transferred, much less sue its parent company.<sup>157</sup>

The second case involves an agreement between the German Railway or Deutsche Bahn AG (DB) and Citibank, which came about as a result of public protest by consumer groups and data protection authorities in Germany.<sup>158</sup> The DB is a monopolist railway that encouraged consumers to use fare cards by offering considerable discounts.<sup>159</sup> The fare cards, called the RailwayCard, were initially produced by another German private company (Bertelsman) and were very popular.<sup>160</sup> In November 1994, the DB entered into a Co-Branding agreement with Citibank to provide the cards with a cash-free payment function, thus making them VISA credit cards to be manufactured in the United States.<sup>161</sup>

Protest by consumer groups and data protection authorities caused DB and Citibank to renegotiate their agreement to make the old style card available again as an option.<sup>162</sup> However, it was widely believed that DB had sold data of its existing and future customers to Citibank.<sup>163</sup> In addition, the German data protection supervisory authorities criticized the application forms for the bank card, which required personal data on creditworthiness, since all the customers really wanted was to get on the train and not to apply for a credit card.<sup>164</sup>

The Berlin Data Protection Commission became involved and made it clear that the data was not to be outsourced to Citibank, as this would result in a massive transborder flow of data of German citizens to a non-EU country.<sup>165</sup> Although Ger-

---

157. *Id.* ("A domestic exporter is even less likely to sue its home office or foreign partner to enforce the terms of an agreement").

158. See Alexander Dix, *Case Study: North America and the European Directive—The German RailwayCard*, Speech at the 18th International Privacy and Data Protection Conference, Ottawa, Canada (Sept. 18-20, 1996) (visited Aug. 28, 1999) <[http://www.datenschutz-berlin.de/doc/int/konf/18/bahn\\_en.htm](http://www.datenschutz-berlin.de/doc/int/konf/18/bahn_en.htm)>.

159. *Id.* at 1.

160. *Id.*

161. *Id.* at 1-2.

162. *Id.* at 2.

163. *Id.* at 2.

164. *Id.*

165. *Id.*

many had not yet adopted the Directive into national law, the Berlin Data Protection Commissioner argued that no such data transfer take place unless the parties complied with articles XXV and XXVI of the Directive.<sup>166</sup> Because both DB and Citibank were interested in continuing their business relationship beyond 1998 when the Directive would be adopted by Germany, they entered into a contractual agreement which was deemed to provide "adequate" protection.<sup>167</sup>

The essential aspects of this contract were, *inter alia*, that both parties agree to apply German Data Protection Law,<sup>168</sup> that customer data only be used for the purpose of manufacturing of the cards,<sup>169</sup> and that the American subsidiary agree to appoint data protection supervisors to ensure that German data protection requirements were adhered to.<sup>170</sup> Significantly, Citibank subsidiaries in the United States also agreed to permit on-site audits by German data protection supervisory authorities, including their nominated agents (such as American consulting or auditing firms).<sup>171</sup> The contract further granted rights to DB customers as third party beneficiaries and held both the German Citibank subsidiaries and DB liable for any violations by Citibank in the United States.<sup>172</sup> Finally, the parties to the contract agreed to submit to the jurisdiction and venue of the courts of Frankfurt am Main, and that the contract would be governed by German law.<sup>173</sup> One can safely conclude, as Deputy Commissioner Dix did, that this contract meets the objectives of the Directive.<sup>174</sup>

Because this contract provides European citizens with

---

166. *Id.*

167. *Id.* at 2-3.

168. See Alexander Dix, *Agreement on Interterritorial Data Protection*, § 1, paras. 3 & 4 (visited Aug. 28, 1999) <[http://www.datenschutz-berlin.de/doc/int/konf/18/intdp\\_en.htm](http://www.datenschutz-berlin.de/doc/int/konf/18/intdp_en.htm)> (stating: "protection shall be governed by the standards as laid down in the German Federal Data Protection Law *Bundesdatenschutzgesetz*").

169. *Id.* § 2, para. 1.

170. *Id.* § 6, paras. 1, 2.

171. *Id.* § 3.

172. *Id.* § 8, paras. 1, 5.

173. See *id.* § 15, para. 3 (stating: "the parties hereto submit to the jurisdiction and venue of the courts of Frankfurt am Main"). See *id.* §15, para. 4 (stating: "This Agreement shall be governed by, interpreted and construed in accordance with German law.").

174. Dix, *supra* note 158, at 4.

adequate data protection and offers remedies, it could be used as a model for other firms to follow in the future. However, even though this contract meets the requirements of the Directive, that is not sufficient to conclude that contracts, in general, provide the correct approach to satisfying the Directive's requirements.

*B. The Shortcomings of the Contractual Approach.*

Although the contractual approach provided an adequate solution to personal data protection in the case involving the DB and Citibank, what must be taken into consideration here is the specific nature of the circumstances leading to this contract, and the nature of the firms who were parties to the contract.

First, both firms are quite large. Citibank is one of the biggest and most well-known financial institutions in the world. DB is, practically speaking, a monopoly controlling the German Railway sector.<sup>175</sup> Moreover, the amount of data involved was large enough to justify contract negotiations between the firms, since there were in excess of 3 million railway cards issued.<sup>176</sup> In addition, Citibank (banking) and DB (public transportation) both operate in sectors that are very heavily regulated. Consequently, both are experienced in dealing with regulations and have regulatory staff to ensure compliance with applicable regulations. Presumably, due to their size and regulatory experience, they are more amenable to audits than most firms.

Further, the contract was developed after there had already been an agreement between German and United States banking supervisory authorities on transborder processing of accounting data, which permitted the incorporation of that agreement into the contract by reference to the applicable laws.<sup>177</sup> Thus, the added step of looking at personal financial data involved in transborder transit for compliance to the Directive, in addition to financial regulatory standards, was likely a significantly smaller burden than for a firm which does not regularly look at data for purposes of regulatory compli-

---

175. See Dix, *supra* note 158, at 1.

176. *Id.* at 2. By July, 1996, 3,054,000 cards had been issued. *Id.*

177. *Id.* at 4. See also Dix, *supra* note 168, § 1.

ance. Another factor that is unique to these firms is that following a change in German law, the Berlin Data Protection Commission had just assumed jurisdiction over DB, and as a result was able to participate in the discussion between DB and Citibank, and presumably help with interpretation of German law to facilitate the contract negotiations.<sup>178</sup> Finally, following the public upheaval after the issuance of the Railway/VISA card,<sup>179</sup> both DB and Citibank had a very strong incentive to reach this agreement.

It is quite unlikely that absent similar circumstances such comprehensive protection can be achieved using a contractual approach. It is probable that smaller firms in non-regulated or minimally regulated sectors would not have the legal resources available to determine the amount of protection necessary to close the gap between the national law and the protection available in the third country. Nor is it likely that the national data protection authority would be able to assist a multitude of firms from various countries with different laws to determine what additional protection is required. As the deputy commissioner of one European data protection authority noted, applying a contractual approach would mean that the data protection authorities would not only have to have familiarity with the level of protection in a given country like the United States, but would have to determine the data protection measures of individuals firms.<sup>180</sup>

Given the complexities of ensuring data protection with the contractual approach, it should be used as an exception and not as a matter of course. In fact, even if there were no inherent difficulties with applying the contractual approach, there is still one overriding reason why the contractual approach is not a desirable long-term solution: it only ensures data protection of European Union citizens. It thus fails to make advances in creating data protection for Americans.

---

178. See Dix, *supra* note 168, at 2, 6.

179. *Id.*

180. See Dix, *supra* note 158, at 6.



## V. PROVIDING PERSONAL DATA PROTECTION IN THE UNITED STATES—SOME OBSERVATIONS

While the primary purpose of this Note was to evaluate the effectiveness of the contractual exception as a means of meeting the requirements of the Directive, some brief observations concerning the implementation of increased data protection rights in the United States seem in order.

With the increased opportunities to misuse personal information made possible by technology, it is imperative that citizens of the United States also enjoy increased privacy protection. While the Directive provides excellent guidance concerning the substantive nature of data protection, it is unlikely that the highly bureaucratic approach used in Europe will find acceptance here, given the American public's general distrust of government and the general laissez-faire attitude of Americans towards business. Thus, an approach must be found that satisfies the spirit of the European Directive and is also compatible with American values.

Because Americans have traditionally been suspicious of big government,<sup>181</sup> intrusions into all areas of private life—be they personal or regarding business—are subject to resistance. Personal data protection is no exception. A 1992 survey by Lois Harris & Associates indicates that 79% of the American public is concerned about threats to personal privacy and 76% feel that they have lost control over their personal information.<sup>182</sup> However, a 1996 survey by Lois Harris & Associates reveals that only 28% favor creation of a government privacy commission.<sup>183</sup> According to this survey "although the public does express concern about how businesses handle personal information, consumers appear more concerned about the actions of government and would prefer to let businesses adopt voluntary policies rather than have the government step in, except where *voluntary* policies have been seen to fail."<sup>184</sup> In view of these

---

181. See generally *supra* Section II.A.

182. LOUIS HARRIS & ASSOCS., HARRIS-EQUIFAX CONSUMER PRIVACY SURVEY 126 (1992). See Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 441 (1995).

183. LOUIS HARRIS & ASSOCS. & ALLAN F. WESTIN, THE 1996 EQUIFAX-HARRIS CONSUMER PRIVACY SURVEY 36 (1996) [hereinafter EQUIFAX-HARRIS]. See also Cate, *supra* note 12, at 33 n.253.

184. EQUIFAX-HARRIS, *supra* note 183, at 37. See Cate, *supra* note 12, at 33 n.253.

sentiments, the establishment of a governmental privacy agency along the lines of the European Directive seems unlikely.

It is also not likely that American businesses are willing to absorb the additional costs involved in complying in a European-style system. These costs are incurred in diverse ways as a result of the two ways European countries have chosen to implement the Directive.

One approach is the registration of any data processing by an institution as required by French and British national law.<sup>185</sup> According to the registration approach, any time data processing is to occur, the institution doing the data processing is required to register it with the appropriate government agency.<sup>186</sup> This register is available for public inspection, permitting the public access to its data from the data processor.<sup>187</sup> Because the Directive requires that the individual be given access to that data, and information about it, without excessive cost or delay,<sup>188</sup> the costs for complying with the Directive can be quite high. National legislation determines the maximum costs that have to be paid by the person making the request.<sup>189</sup> In the U.K., that cost is limited to ten English pounds (roughly fifteen U.S. dollars), whereas the German Act provides for free access to the information.<sup>190</sup> The British Bankers' Association has estimated the cost of one institution providing one customer with "a simple straightforward report" containing the information required by the Directive to be greater than 150 English pounds (roughly 225 U.S. dollars) and concluded that the cost for a major bank to comply with the Directive "runs into millions."<sup>191</sup> Perhaps the most impressive example of the seriousness of the registration requirement is found under French law, "where the use of personal data for reasons other than that set out in the . . . registration is punishable by criminal penalties."<sup>192</sup>

---

185. See Wuermeling, *supra* note 63, at 454.

186. *Id.* at 453-54.

187. See Directive, *supra* note 11, art. 12.

188. *Id.* art. 12(1).

189. See Wuermeling, *supra* note 63, at 446 nn.170-71.

190. *Id.* at 446.

191. Cate, *supra* note 12, at 15 (citing The Home Office Consultation Paper on the implementation of the EU Data Protection Directive—The British Bankers' Association Response, at 48-49).

192. Schwartz, *supra* note 13, at 492 n.150.

The other approach taken to comply with the Directive, in lieu of public registration, is to require private oversight. While public institutions in Germany are required to use registration, the oversight approach is generally used for private companies.<sup>193</sup> Under this principle each firm provides its own oversight staff in the form of a data protection commissioner who is an employee of the company.<sup>194</sup> If the company has more than five persons working on computers, one person must be appointed to be in charge of data protection.<sup>195</sup> Large companies employ a full-time data commissioner while small businesses assign that function to an individual who has additional responsibilities.<sup>196</sup>

Considering the traditional distrust of government in the United States, the oversight approach may not be embraced initially. It would permit the creation of a relatively small governmental agency whose role would be to work with industry in creating the necessary regulation to protect the privacy expectations of the American public. However, the majority of persons involved would be personnel of private industry, thus giving the entire approach a self-regulatory aspect. If this approach fails to achieve the desired results, lawmakers could still pass legislation necessary to achieve adequate results on the basis of their experience with a semi-self-regulatory approach.

An alternative to legislation and the creation of a privacy agency would be to treat private information as property, akin to intellectual property. Although the right to private information as such does not exist, it bears noting that the appropriation of one's name or likeness for commercial gain,<sup>197</sup> now also known as the right to publicity, was not thought to be a right in *Roberson v. Rochester Folding Co.*<sup>198</sup> in 1902. However, by 1905 this right was accepted in *Pavesich v. New England Life Insurance Co.*<sup>199</sup> It was the advent of photography and lithog-

---

193. See Wuermeling, *supra* note 63, at 454 (citing SCHAFFLAND & WILTFANG, BUNDESDATENSCHUTZGESETZ §§ 26(5), 18(2), 32 (1995), and citing Eickeler, HANDELSBLATT, Nov. 12, 1992, at 4).

194. *Id.* at 456.

195. *Id.* at 457.

196. *Id.*

197. See *supra* Section II.A.

198. 64 N.E. 442 (N.Y. 1902).

199. 50 S.E. 68 (Ga. 1905).

raphy which made possible the capturing of one's exact likeness and the duplication of that image innumerable times that formed the underpinnings of the right to publicity.

Just as advances in technology changed the legal paradigm concerning the right to one's name or likeness and thus created the recognition in one's property interest in the right to publicity, so the advent of biotechnology, and mass storage and processing, may change the legal paradigm applicable to personal information. The law may not necessarily recognize the right to personal data as such, anymore than the right of publicity was recognized in the absence of commercial gain. However, the law may in the future recognize a corollary right—the right not to have one's personal data distributed to one's economic disadvantage in the absence of permission to do so. This approach would at least address the commercial aspects of one's personal data.

The right to avoid the "appropriation of one's personal data" could cover such sensitive areas as disclosure of medical or genetic information which would disadvantage one in obtaining insurance and employment, or the sale of personal information for marketing use. Personal information is often only valuable when it exists in large quantities. Direct Marketing is such an example. Therefore, it may be argued that privacy rights will be under-enforced because there are insufficient damages to justify legal action. However, if suits can be certified as class actions, there would be sufficient incentive. Finally, in particularly egregious cases, the courts should be encouraged to permit punitive damages to curb the misuse of personal data in the future.

## VI. CONCLUSION

While the Directive may promise to protect the personal data of Europeans within Europe, the contractual approach stipulated by Article 26 of the Directive has been criticized as a solution for ensuring that a European citizen's personal data will not be misused in non-Member States. Additionally, because the effectiveness of the provision depends on the nature of the data exporters and data importers, the contractual solution is at best a short-term solution. Since the European data protection authorities are encouraged by the Directive to examine the adequacy of protection on a case-by-case basis, compa-

nies for whom the contractual approach presents a less than ideal solution, may still choose to use it as a demonstration of a good faith effort to the data protection authorities that they intend to protect European citizen's privacy.

Although the contractual approach is useful in aiding data importers in the United States to comply with the Directive, a different solution which protects the privacy rights of Americans must be implemented since technological developments will make individuals increasingly more vulnerable to personal data abuse. It would be contrary to the most deeply held values of American society if immutable characteristics, such as genetic information, were used to discriminate against individuals and thus limit their aspirations and potential. If such protections are not guaranteed, the protagonist in *Gattaca*,<sup>200</sup> who was denied the opportunity to achieve his potential because of unfavorable genetic information, will no longer be fiction, but reality.

While the call for the implementation of data privacy regulation may appear premature,<sup>201</sup> a reflection on a quote by Justice William O. Douglas may suggest otherwise:

As nightfall does not come all at once, neither does oppression. In both instances, there is a twilight when everything remains seemingly unchanged. And it is in such twilight that

---

200. GATTACA, *supra* note 6 (The protagonist in the film is determined to be genetically inferior at his birth and is expected to have a short life span. As a consequence, he is denied the ability to pursue his dreams. He subsequently assumes the identity of a genetically superior person, who has been crippled in an accident. Once he assumes this false identity, the protagonist is able to accomplish everything he set out to achieve, but was denied to attempt because of his genetic profile.).

201. That regulation is premature is certainly the view of the Clinton Administration. In a panel discussion of the Directive entitled *The Internet and Public Policy: Who's in Control?*, the Senior Advisor to the President for Policy Development, Ira C. Magaziner stated: "We made clear to the European Union, we do not accept their approach to this . . . [T]he kind of government regulation that they're advocating is too bureaucratic, too regulatory, will stifle a great deal of the activity on the Internet, and we're not going to do that in this country." *The Internet and Public Policy: Who's in Control? A Panel Presented by the New York New Media Association*, FED. NEWS SERVICE, June 12, 1998, available in LEXIS, News Library, Fednew File. He further expressed the hope that self-regulation would accomplish the goals of the Directive, but if self regulation failed, the issue would be subject to further review. What was clear was that the Clinton Administration would not tolerate blockage of data flows by the European Union: "[I]f the European Union tried to impose their system on us, and tried to block data flows . . . we'd absolutely protest to the WTO, as blocking trade flows." *Id.*

we all must be most aware of change in the air—however slight—lest we become unwitting victims of the darkness.<sup>202</sup>

*Michael W. Heydrich*

---

202. Letter from William O. Douglas to Young Lawyers Section of the Wash. State Bar Ass'n (Sept. 10, 1976), in *THE DOUGLAS LETTERS* 162 (Melvin Urofsky ed. 1987).

