

THE EU – U.S. PRIVACY CONTROVERSY:  
A QUESTION OF LAW OR GOVERNANCE?

A THESIS  
SUBMITTED TO THE  
STANFORD PROGRAM IN INTERNATIONAL LEGAL STUDIES  
AT THE STANFORD LAW SCHOOL,  
STANFORD UNIVERSITY  
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF  
JURIDICAL SCIENCES MASTER

By

Roland Vogl

May 2000

## **ABSTRACT**

The EU and the US are at a deadlock over different levels of privacy protection. The two sides have made cooperative efforts to bridge the gap between their diverging privacy regimes without satisfaction. This paper will review the sources of conflict in the controversy over privacy protection. This thesis will argue that the international debate has failed to provide a viable solution because it fails to address the real source of conflict. It has been assumed that the conflict is due to substantially divergent legal traditions. At a first glance the reason for the dispute appears obvious: One system (EU) considers privacy rights to be fundamental human rights, the other system (US) considers privacy rights to be a tradable commodity. However, this paper argues that the conflict is caused by different governance traditions, not legal traditions. In other words, privacy regimes reflect fundamental different visions of governance in a society. Therefore, even if basic principles are shared between the EU and the US, when these principles are implemented at a domestic level they inevitably lead to different levels of protection.

This thesis further argues that a solution to the privacy problem is challenged by rapid technological developments, and domestic privacy debates. This paper concludes that international co-operation on how to protect privacy is the right path, but that only an effort to address the difference in governance philosophies will provide a functional solution.

## PREFACE AND ACKNOWLEDGEMENTS

This project started more than a year ago when I decided to combine my strong interest in international relations and legal aspects of communication into a thesis proposal for the Stanford Program in International Legal Studies. Coming from a European perspective I found it striking and fascinating that a country like the United States could not share the European tradition of perceiving of privacy as a fundamental human right. The nine months that I fully immersed myself in the privacy debate helped me understand the multiple dimensions of this debate. As overwhelmingly diverse as this theme is, I think I could not have picked a topic that would have provided me with more insights about U.S. society than the privacy debate. Further it taught me a lot about my own cultural background.

I am greatly indebted to my primary advisor Professor Sophie Pirie for her continuous support, insights, encouragement, patience and probing criticisms and her willingness to listen to non-academic issues. I would also like to thank Carey Heckman, my specialized advisor for his insightful comments, advice and suggestions.

Both Carey and Sophie are leaving Stanford Law School. I feel privileged to have had the opportunity to work with them.

I gratefully acknowledge the generous editorial help to part of this paper from Adriana Camarena and the professional editorial guidance from Professor Phil Hubbard.

I am greatly indebted the Austrian Ministry of Science, and the Tyrolean government that enabled my study with generous financial support.

I myself, however, remain wholly responsible for the views and the errors herein.

Last but not least, I would like to extend my appreciation to my colleagues in the SPILS program who provided me with the emotional stamina and plenty of precious new insights.

## TABLE OF CONTENTS

INTRODUCTION .....	1
I. THE EU - U.S. PRIVACY CRISIS .....	3
A. BACKGROUND.....	3
1. The EU Data Protection Directive and the New International Privacy Debate .....	3
a) Transborder Dataflows and the Directive’s Requirement of “Adequate” Protection .....	4
b) The Specter of Article 25 .....	6
2. The Search for a Compromise .....	7
a) The U.S. Seeking “Adequacy” .....	7
b) The Safe Harbor Deal and Persisting EU Skepticism.....	9
c) The Current State of Affairs .....	11
d) Conclusion.....	13
II. CLASHING PRIVACY REGIMES IN A WORLD OF SHARED PRIVACY PRINCIPLES.....	16
A. INTRODUCTION.....	16
B. CONVERGENCE ON INTERNATIONALLY AGREED BASIC PRIVACY PRINCIPLES .....	18
1. The U.S. National Information Infrastructure Privacy Principles .....	18
2. EU Principles.....	20
a) EU Principles Converging with Basic Principles .....	20
3. Fundamental Right Approach v. Market Oriented Approach.....	22
C. SUBSTANTIAL DIVERGENCE OF IMPLEMENTATION REGIMES.....	24
1. Background .....	24
2. The U.S. Privacy Regime .....	25
3. The EU Privacy Regime .....	31
4. Applying the Diverging Regimes: A Case Study About Online Profiling .....	34
a) Introduction .....	34
b) What is Online Profiling.....	34
c) Online Profiling and the U.S. Privacy Regime .....	37
i. No Handle on Online Profiling Under U.S. Privacy Laws .....	37
ii. Self-regulatory Programs, Privacy Seals .....	38
d) Online Profiling Leaves the EU Data Protection System Scrambling.....	42
5. Most Substantial Divergence on Protection of Secondary Use of Data, Sensitive Data and Enforcement .....	44
D. DIFFERENT GOVERNANCE CHOICES THE DRIVING FORCE BEHIND DIFFERENT PRIVACY REGIMES.....	46
1. U.S. Privacy Concepts Reflecting Governance Choices .....	46
2. The Evolution of the European Privacy Paradigm and the Distinctly European Context .....	48
E. CONCLUSION .....	50
III. AN APPROACH TO AVOID FUTURE CLASHES OF PRIVACY REGIMES IN A GLOBAL CONTEXT .....	53
A. INTRODUCTION.....	53
B. THE IMPACT OF THE EU – U.S. CONTROVERSY ON INTERNAL PRIVACY DEBATES .....	54
1. U.S. Policy Debate .....	54
a) U.S. Privacy Advocates .....	55
b) U.S. Industry.....	57
c) U.S. Policymakers .....	59
d) U.S. Public View .....	60
2. EU Internal Debate .....	61
a) Privacy Advocates .....	61
b) Businesses .....	62
3. Conclusion.....	63
C. HOW TO REACH INTERNATIONAL CONSENSUS? .....	64
1. Structural Pitfalls.....	64

2. Promising Alternatives .....	66
3. Intergovernmental Players and Technical Standard Bodies Can Push Forwards .....	69
a) Introduction .....	69
b) OECD/Council of Europe.....	69
c) WTO.....	71
d) Technical Standard Bodies Enabling Harmonization in an Online Context.....	72
4. International Harmonization Through Technical Codes.....	73
5. International Harmonization Through New International Information Privacy Instruments? .....	76
D. CONCLUSION.....	80
BIBLIOGRAPHY .....	82

## INTRODUCTION

New information technologies are challenging privacy regimes around the world. They empower different types of actors to exercise practices that infringe on the personal privacy of individuals. Since these technologies are borderless, infringement is also borderless. Exploding transborder data flows have brought privacy regimes to clash over the level of protection that should be guaranteed to citizens of their respective countries. Differences in privacy standards around the world create enormous uncertainty for individuals and businesses.

In the course of this thesis I will focus on the recent EU and U.S. controversy over different forms of privacy protection. In order to move toward a viable future way to deal with privacy, capable of dealing with challenges of technology and globalization, I will analyze a number of critical issues.

The clash of the two privacy regimes is often attributed to conflicting concepts and the according principles of privacy protection. In the course of this paper, however, I will argue that the core reason for the clash are largely different systems of implementation of many shared basic principles and national policies interpreting basic principles quite differently. Ultimately this will lead me to the conclusion that the core reason for the international divergence are different visions of governance.

In Part I of this thesis, I will analyze the political controversy and a recently proposed policy instrument aimed at creating a bridge between the two conflicting regimes. In Part II, I will show that there is large convergence on international privacy principles – an insight that surprises in light of the seemingly unreconcilable privacy regimes. At the same time I will show that this convergence is defeated when common

principles are fed into national implementation systems - as I will illustrate by means of a short case study on “online profiling.” I will further show that there are deeper reasons and political forces that are responsible for the diverging implementation regimes. These reasons can be found in different visions of governance.<sup>1</sup>

Finally in Part III, I will examine the national privacy debates and the role that international institutional players and technical standard bodies will play in the search for international consensus. I will argue that international players will be key in a future privacy debate.

---

<sup>1</sup> Joel Reidenberg has laid out this argument succinctly in a forthcoming article. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 55 STAN. L. REV (forthcoming May 2000). Draft manuscript of Reidenberg’s article on file with author of this thesis.

# **I. THE EU - U.S. PRIVACY CRISIS**

## **A. BACKGROUND**

### **1. The EU Data Protection Directive and the New International Privacy Debate**

On October 24, 1998 the EU Data Protection Directive<sup>2</sup> went into force. From that day on the U.S. approach to privacy protection has been at the focus of a hefty political controversy between the U.S. and the EU. The main cause for this dispute is that the EU views the standard of protection of personal data that the U.S. privacy regime as insufficient to protect EU citizens' data.

Both privacy regimes represent two extremes on a "privacy protection scale." The EU Directive promulgated a unified and comprehensive data protection regime for the fifteen EU member countries and its 370 million people. The obligations and rights laid down in the Directive build upon those laid down in the Council of Europe's Data Protection Convention (1981)<sup>3</sup>, which in turn are similar to those included in the OECD guidelines (1980)<sup>4</sup> and the UN guidelines (1990)<sup>5</sup>. Designed to further the creation of the EU internal market<sup>6</sup>, the Directive requires all member states to devise national laws to meet its minimum standards for protecting the privacy of personal information. In

---

<sup>2</sup> Directive 95/46/EC of the European Parliament and of the Council of 24<sup>th</sup> October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, <[http://europa.eu.int/eur-lex/en/lif/dat/1995/en\\_395L0046.html](http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html)>.

<sup>3</sup> COE, Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur.T.S.No. 108 <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/inter/con10881.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm)>.

<sup>4</sup> OECD, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data <<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>>.

<sup>5</sup> UN Guidelines Concerning Computerized Personal Data Files <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/inter/un.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/un.htm)>.

addition, the creation of Directive 95/46/EC reflects the most profound structural change in the history of the European Union, namely the transition from a merely economic union to a decidedly political one. The paramount aim has become a Union characterized, in the terms of the Maastricht Treaty, by the abolition of internal frontiers, the establishment of an economic and monetary union, the acknowledgment of a common citizenship, the implementation of a common foreign and security policy, and intensive cooperation in the fields of justice and home affairs.<sup>7</sup> Consequently, the EU privacy regime also reflects a typical European pattern, namely a great amount of centralization and coordination of government authority, even at a supranational level.

By contrast, the current U.S. privacy regime is complex and highly decentralized.<sup>8</sup> It can be best characterized as a complex fabric of sectoral regulation, at both federal and state levels<sup>9</sup> combined with industry self-regulation in numerous areas. There are numerous statutes and regulations on privacy related issues. Enforcement is sought by various state and federal agencies charged with oversight of other industries.<sup>10</sup>

**a) *Transborder Dataflows and the Directive's Requirement of "Adequate" Protection***

The EU Directive insists on a free flow of information within the European Union. EU Member States are no longer allowed to ban flows of information to other Member States. In order to protect transfers of personal data among Member States the Directive

---

<sup>6</sup> Directive 95/46/EC, findings (1) to (9).

<sup>7</sup> See Spiros Simitis, *From the Market to the Polis: The EU Directive on The Protection of Personal Data*, 80 IOWA L. REV. 445, 447 (1995).

<sup>8</sup> See, e.g., Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, at 3 (1998).

<sup>9</sup> There is also a variety of sectoral legislation on the state level that may give additional protections to citizens of individual states. See ROBERT ELLIS SMITH & PRIVACY JOURNAL, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1997 ed.).

<sup>10</sup> As New York Times correspondent Edmund L. Andrews puts it: the U.S. regulation of data privacy consists of a "hodgepodge of statutes and regulations enforced by various state and federal agencies

requires an equivalent minimum standard of protection.<sup>11</sup> For that purpose it sets out detailed requirements for harmonizing Member States' data protection laws.

The Directive imposes significant restrictions on most data collection, processing, dissemination, and storage activities, not only within Europe, but throughout the world if the data originates in an EU Member State. Unlike the Council of Europe Convention, the Directive contains explicit provisions concerning the conditions of transfers to non-member Nations. Article 25 of the Directive prohibits the transfer of personal data – defined as any information relating to an identified or identifiable natural person ('data subject')<sup>12</sup> – out of EU territory unless the other country meets EU standards for "adequate" data protection.<sup>13</sup> The rationale supporting the long arm approach of these rules on transborder data transmissions is that promulgating a Directive with high protection standards would make little sense if those handling EU citizens' personal data outside Europe could systematically violate the privacy rights protected under the Directive.<sup>14</sup> The EU Commission apparently sought to avoid countries becoming data havens, allowing the practices Europe prohibits. For instance, businesses in the data havens might compile secret dossiers or conduct intrusive marketing practices by mail, telephone, or e-mail.<sup>15</sup>

---

charged with oversight of other industries." Edmund L. Andrews, *European Law Aims to Protect Privacy of Personal Data*, N.Y. TIMES, Oct. 26, 1998, at A1.

<sup>11</sup> The Directive states: "Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all the Member States," Directive 95/46/EC pmbl. at para (8).

<sup>12</sup> See Directive 95/46/EC, art 2(a).

<sup>13</sup> See Article 29 Working Party, Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions between the European Commission and the United States Government, (Jan. 26, 1999) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp15en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp15en.htm)>.

<sup>14</sup> See SPIROS SIMITIS, § 1 IN KOMMENTAR ZUM BUNDESDATENSCHUTZGESTZ 77-78 (Spiros Simitis et al. eds., 1992).

<sup>15</sup> PETER SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS 26 (1998).

***b) The Specter of Article 25***

A group consisting of European Data Protection Commissioners was set up under the Directive's Article 29 in order to oversee the implementation of the Directive ("Working Party on the Protection of Individuals with Regard to the Processing of Personal Data" or "Article 29 Working Party"). Reflecting the typical European preference for comprehensive government regulation, the "Article 29 Working Party" noted in various opinions that the patchwork of narrowly focused sectoral laws and industry self-regulation presently in place in the United States cannot be relied upon to provide adequate protection for personal data transferred from the European Union.<sup>16</sup> The Working Party's recommendations and opinions have a central role in developing the application of Article 25 that basically enables EU decision-makers to cut off the flow of information from Europe to other countries.<sup>17</sup> Hence, this provision empowers the EU to impose "data embargos" on countries that are not complying with the EU's standards for adequate protection.<sup>18</sup>

Data embargos are not an entirely new pattern in the international privacy debate. In the late 1980s, for example, France threatened Italy, which until the passage of the Directive had no general data protection legislation, with cutting off transfers of certain personal information. In the particular dispute, Fiat-France eventually entered into a contract with Fiat-Italy, which required offering the protection of French law to the

---

<sup>16</sup> See, e.g., Article 29 Working Party, *supra* note 13.

<sup>17</sup> Article 25(4) Directive 95/46.

<sup>18</sup> Of course a country affected by such a move could decide to bring such a conduct to the World Trade Organization, some American experts predicted though that the Europeans would be likely to win in such a case. See P. Swire cited in Declan McCullagh, *US Twitchy on EU Data Privacy*, WIREDNEWS (Oct. 16, 1998), <<http://www.wired.com/news/news/business/story/15671.html>>.

information once transferred to Italy.<sup>19</sup> This model of using a privately entered agreement to substitute for the absence of data protection laws, has been revisited in the search for a general solution between the EU and the U.S.

## 2. The Search for a Compromise

### a) *The U.S. Seeking “Adequacy”*

Given that the European Union is the U.S.’s largest trading partner EU officials have considerable bargaining leverage over the issue. In 1997, the United States exported \$253.6 billion of goods and services to the European Union and imported \$270.3 billion of goods and services from the European Union.<sup>20</sup> Transatlantic trade is dwarfed by sales of U.S.-controlled affiliates based in Europe. Over half of all the foreign production of goods and services of U.S. companies is produced by U.S. affiliates in Europe.<sup>21</sup> In light of these figures, U.S. retaliation against the EU for placing information flow bans could give rise to a more severe trade counter-retaliation seriously harming U.S. commercial interests. In such a case, affected U.S. companies would most probably press the U.S. government to accommodate EU demands in order to regain access to the EU market.<sup>22</sup>

Given the high stakes on both sides and the tension that evolved between both players, EU chief negotiator Mogg at one point went so far as to speak about the risk of a

---

<sup>19</sup> See Paul Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 491, at 492 (1995).

<sup>20</sup> This was out of a total of \$690 billion of U.S. exports. See *Issues in U.S.-European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy Before the House Committee on International Relations*, Federal News Services (May 7, 1998) (testimony of Franklin Vargo, Assistant Secretary of Commerce).

<sup>21</sup> See U.S. Department of Commerce, *Foreign Trade Data*, <<http://www.ita.doc.gov/td/industry/otea/usftd/>>.

<sup>22</sup> See Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT’L L. 1, at 39 (2000).

trade war.<sup>23</sup> Such a trade war over privacy seems improbable, though, given that the U.S. market is also the largest foreign market for EU firms. Accordingly, European commercial interests would also press EU Member State representatives and EU officials to avoid a transatlantic trade war over data privacy issues.

Driven by the mentioned commercial and political interests, the U.S. Department of Commerce (DOC) issued in November 1998 the first draft of the so-called “International Safe Harbor Privacy Principles” (“Safe Harbor Principles”).<sup>24</sup> The key idea of the Safe Harbor approach is to provide joining organizations with a presumption of adequacy in order to ensure the continuation of data transfers from the EU.

According to the first draft of the Safe Harbor Principles, U.S. organizations could meet the requirements by self-certifying that they adhere to the Safe Harbor Principles. The decision to join the Safe Harbor would be entirely voluntary. Compliance with the Safe Harbor Principles would rely on a combination of private-sector dispute resolution mechanisms and U.S. law - such as Section 5 of the FTC Act - which forbids unfair and deceptive acts (e.g. posting a privacy policy and not abiding by it).

On the EU side, the Safe Harbor Agreement would be met by a decision under Article 25(6) of the Directive certifying that the Safe Harbor Principles represented a standard of “adequate protection.” Such a decision would provide that “data controllers” in the EU can transfer personal data to U.S. based organizations that qualified for the

---

<sup>23</sup> See Declan McCullagh, *Safe Harbor Swimming in Circles*, WIREDNEWS (Apr. 29, 1999) <<http://www.wired.com/news/news/politics/story/19414.html>>. The European Union has delayed enforcing the EU Directive’s provisions on third-country transfers while negotiations take place. See G. Shaffer, *supra* note 22, at 44-45.

<sup>24</sup> See U.S. Department of Commerce, Draft International Safe Harbor Privacy Principles as of Nov. 4, 1998 (hereinafter: “November Draft”) <<http://www.ita.doc.gov/ecom/aaron114.html#Safe>>. Latest draft (Mar. 2000): <<http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm>>. The Department of Commerce created these principles under its statutory authority to foster, promote, and develop international commerce.

Safe Harbor. One effect of such a decision would also be that any Member State law requirements for the prior authorization of transborder data transfers would be waived, or that approval would be automatically and promptly granted with respect to transfers to organizations qualifying for the Safe Harbor.

An “adequacy decision” would create a presumption of adequate privacy protection for U.S.-based organizations that self-certify their adherence to the Safe Harbor Principles and are subject to the jurisdiction of the U.S. Federal Trade Commission or other body with similar statutory powers.

***b) The Safe Harbor Deal and Persisting EU Skepticism***

The first draft of the Safe Harbor Principles<sup>25</sup> contained provisions on notice, choice, onward transfer, security, data integrity and enforcement. According to the initial draft, businesses could have qualified for the Safe Harbor in different ways: One was to join private sector developed privacy programs – such as TRUSTe<sup>26</sup> or BBBOnline<sup>27</sup> - that adhered to the Principles. A second way was if an organization was already subject to U.S. statutory, regulatory, administrative or other body of law<sup>28</sup> that also effectively protect personal data privacy. A third way was for business organizations to put in place the safeguards deemed necessary by the EU, by incorporating the Safe Harbor principles into agreements entered into with parties transferring personal data from the EU<sup>29</sup> – very much alike the earlier mentioned case of Fiat France and Fiat Italy.

---

<sup>25</sup> See U.S. Department of Commerce, November Draft *supra* note 24.

<sup>26</sup> See <<http://www.truste.org/>>.

<sup>27</sup> See <<http://www.bbbonline.com/>>.

<sup>28</sup> Or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a municipal securities rule-making board.

<sup>29</sup> See U.S. Department of Commerce, November Draft, *supra* note 24.

The Article 29 Working Party expressed a number of substantial concerns about the first as well as all subsequent drafts.<sup>30</sup> It criticized specifically that the decision to adhere to the set of principles should belong solely to the individual U.S. company. In this case the problem of those companies which do not wish to apply the principles would continue to exist as long as no comprehensive legislation existed.<sup>31</sup>

Faced with the subsequent refusal of the first draft, the Department of Commerce issued the revised Safe Harbor Principles and a set of “Frequently Asked Questions” (FAQs)<sup>32</sup> at the end of April 1999.<sup>33</sup> Yet, along with the EU Commission, some U.S. privacy experts<sup>34</sup> criticized the revised draft for being still too vague and too loose on sanctions. The Article 29 Working Party particularly stressed that the draft overall lacked

---

<sup>30</sup> See Article 29 Working Party, Opinion 1/99, *supra* note 13.

<sup>31</sup> Further, the Working Party was concerned that the provisions on consumer access to data kept about them allowed data processors too much hedging room. In addition, the Working Party pointed out that the purpose specification principle of the OECD Privacy Guidelines is absent, and is only partly replaced by a “choice” principle which in effect allows data collected for one purpose to be used for another, provided individuals have the possibility of opting out. The Working Party also noted that proprietary data and any manually processed data are entirely outside of the scope of the U.S. principles, while the “choice” principle provided no protection to data collected from third parties and the “access” principle excludes public record-derived information. Finally, the Working Party showed that, according to the third paragraph of the introduction of the principles, adherence to the principles is subject to a number of exceptions and limitations such as “risk management” and “information security” - all notions that according to the Working Party are too vague and open-ended. See Article 29 Working Party, Opinion 1/99, *supra* note 13.

<sup>32</sup> See Department of Commerce, November Draft, *supra* note 24. The FAQs were intended as a supplement to the Safe Harbor Principles to provide U.S. organizations additional guidance on some aspects of how the principles were supposed to be applied in specific circumstances. See Ambassador Aaron, *Letter on Frequently Asked Questions from Ambassador Aaron* (Apr. 30, 1999), <<http://www.ita.doc.gov/td/ecom/aaron430.htm>>.

<sup>33</sup> In the revised draft the definition of personal data referred to an identified or identifiable individual; the exceptions to the principles appeared more coherent and in part reflect those envisaged in the Directive. Expressions such as “risk management”, “information security,” and “proprietary data” were omitted. More specifically in the “Notice” Principle the individual was now to be informed of a change of purpose; sensitive information was now fully defined in Principle 2 (“Choice”); and onward transfers now differentiated between transfers amongst organizations adhering to the principles and transfers to third parties outside the safe harbor scheme. See Article 29 Working Party, Opinion 2/99 on the Adequacy of the “International Safe Harbor Principles” issued by the US Department of Commerce on 19th April 1999, (May 3, 1999) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp19en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp19en.htm)>.

<sup>34</sup> See, e.g., Joel Reidenberg cited in James Glave, *US, EU Still Stuck on Privacy*, WIREDNEWS, (Apr. 21, 1999) (visited May 7, 2000) <<http://www.wired.com/news/news/politics/story/19232.html>>.

remedies for victims and efficient enforcement mechanisms.<sup>35</sup> Thus, it concluded that the principles in their June 1 version did not fulfil the requirements of adequate protection.<sup>36</sup>

*c) The Current State of Affairs*

On November 16, 1999 the third draft of the principles and FAQs was published.<sup>37</sup> In the course of the following communications between the EU Commissions services and the Department of Commerce, John Mogg issued a draft Article 25 (6) adequacy decision. Mogg reminded, though, that this decision only refers to the Safe Harbor Principles including the FAQs and not to the U.S. as a whole.<sup>38</sup> Still, the negotiations seemed to be close to a conclusion at the end of November 1999.<sup>39</sup> However, contrary to

---

<sup>35</sup> In particular the Working Party noted that the principles on notice (Principle 1), choice (Principle 2), onward transfer (Principle 3) and access (Principle 6) all lack clarity and concreteness. In addition, the enforcement provision (Principle 7) was criticized for not establishing the rules to be followed for the verification of compliance and for not indicating which authorities can enforce the principles. With respect to the FAQs, the Working Party took the position that they should have authoritative status provided that they are consistent with, and thus considered together with, the Safe Harbor Principles. In addition to that the Working Party stressed that the status of the newly adjunct FAQs had not been clearly indicated. *See* Article 29 Working Party, Opinion 2/99, *supra* note 33. *See* Article 29 Working Party, Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles," (Jun. 7, 1999) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp21en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp21en.htm)>.

<sup>36</sup> Concerning the access principle, it pointed out that it considered the exemptions as contained in the FAQs to be too broad, that public data needs to be covered and that data processed in violation of the principles should be corrected or deleted. Article 29 Working Party, Working Document on the Current State of Play of the Ongoing Discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles," (Jul. 7, 1999), <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp23en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp23en.htm)>. *See also* Joint Report on the Data Protection Dialogue to the EU/US Summit, (Jun. 21 1999) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/news/summit.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/news/summit.htm)>.

<sup>37</sup> *See* U.S. Department of Commerce, November draft, *supra* note 24.

<sup>38</sup> The effect of the decision is therefore limited to those U.S. organizations within the Safe Harbor. The U.S. side has requested that the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act of 1999 also be found to provide adequate protection for the organizations or activities falling under their provisions, but the Commission has reserved its position on this request, pending the examination of further information concerning these acts. *See* EU Commission, Summary of the Main Operative Provisions of a Possible decision on the Basis of Article 25 (6) of the Data Protection Directive Concerning the US "Safe Harbor," (November 1999) <<http://www.ita.doc.gov/td/ecom/256summary1199.html>>.

<sup>39</sup> At the Bureau of National Affairs' (BNA, <<http://www.bna.com>>) "Public Policy Forum on E-Commerce and Internet Regulation" from November 15, 1999 both U.S. and EU officials announced that they expect a final agreement in principle during the U.S. - EU summit in Washington, in December 1999 in Washington. *See* Jennifer L. Alvey, *Coming Soon to a Web Site Near You: Europe's Data Privacy*

the initially fairly optimistic predictions of John Mogg<sup>40</sup>, the Working Party concluded that the revised Safe Harbor Principles still remained unsatisfactory.<sup>41</sup> Thus the agreement on the Safe Harbor was delayed again until March 2000.<sup>42</sup> Then, in March 2000 the media reported that the two sides had finally resolved their controversy and agreed on the Safe Harbor Principles.<sup>43</sup> This final package<sup>44</sup> allows U.S.-based companies not already

---

*Protection Policy*, BNA ELECTRONIC COMMERCE & LAW REPORT, (Nov. 24, 1999)  
<<http://www.bna.com/e-law/>>.

<sup>40</sup> See Letter from John Mogg, Data Protection: Draft of the Commission side of the Exchange of Letters with the US Department of Commerce, (November 1999)  
<<http://www.ita.doc.gov/td/ecom/EULetter1199.html>>.

<sup>41</sup> In its Opinion 7/99 the Working Party therefore pushed the Commission to urge the U.S. side to make a number of key improvements. The Working Party highlighted the following points to be addressed before the Safe Harbor can be viewed as providing adequate protection: clarifying the scope of the Safe Harbor and in particular removing any possible misunderstanding that U.S. organizations can choose to rely on the Safe Harbor principles in circumstances when the Directive itself applies; providing more reliable arrangements allowing Safe Harbor participants to be identified with certainty and avoiding the risk that Safe Harbor benefits will continue to be accorded after Safe Harbor status has, for one reason or another, been lost; making it absolutely clear that enforcement by an appropriately empowered public body is in place for all participants in the Safe Harbor (in its working document of 7 July 1999, the Working Party had already asked the DOC for clarification on the two specific points: First, as regards the treatment of sectors that would be excluded from the scope of the Safe Harbor because they do not fall within the jurisdiction of an FTC-type public body - e.g.: employees data, non-profit sector).

The Working party refers to the FTC Chairman's letters of Sept. 23, 1998 and Nov. 1, 1999. According to these letters, it is clear that the FTC's jurisdiction covers unfair and deceptive acts only if they are "in or affecting commerce." This seems to exclude most of the data processed in connection with an employment relationship (FAQ 9) as well as the data processed without any commercial purpose (e.g.: non-profit, research). Secondly, the Working Party sought clarification with respect to activities, which may be excluded by the organization qualifying for the Safe Harbor as a matter of business choice. As regards this point, the Working Party noted that FAQ 6 invites organizations to indicate the activities of the organization covered by its Safe Harbor commitments. This implies that the same organization could enter the Safe Harbor with one foot and keep the other foot out of the Safe Harbor. Accordingly, the Working Party took the view that this creates legal uncertainty (in particular with regard to data sharing within an organization). Further the Working Party required to make it the rule that private sector dispute resolution bodies must refer unresolved complaints to such a public body. In addition, the Working Party urged the Commission to make the allowed exceptions and exemptions less sweeping and less open-ended, so that exceptions apply only where and to the extent necessary, and are not general invitations to override the principles, a condition that is particularly important as regards the right of access. Finally the Choice principle, which is the lynchpin of the U.S. approach, should be strengthened. See Article 29 Working Party, Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15. and 16. November 1999 by the U.S. Department of Commerce, (Dec. 3, 1999)

<[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp27en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp27en.htm)>.

<sup>42</sup> See Elizabeth de Bony, *EU and U.S. Extend Data Privacy Negotiations*, COMPUTERWORLD, (Dec. 20, 1999) <<http://www.computerworld.com/home/news.nsf/all/9912201privacy>>.

<sup>43</sup> See, e.g., Jeri Clausing, *Europe and U.S. Reach Data Privacy Pact*, N.Y. TIMES, (Mar. 15, 2000)  
<<http://www.nyt.com>>.

<sup>44</sup> The revised Safe Harbor Principles, attending FAQ documents and cover letter inviting public comment from Ambassador David Aaron are currently available at: <[www.ita.doc.gov/td/ecom/menu1.html](http://www.ita.doc.gov/td/ecom/menu1.html)>.

subject to sector-based privacy laws to choose between formal oversight by EU regulators or qualifying self-regulatory regimes enforced by the Federal Trade Commission. The agreement grants the FTC authority to enforce voluntary privacy agreements between U.S. companies and parties transferring data from the EU.<sup>45</sup>

*d) Conclusion*

In my opinion the controversy is far from being resolved. In fact, the Article 29 Working Party was extremely skeptical about the last version of the Safe Harbor Principles in March 2000 and the Article 31 Committee, a committee of Member State representatives that has to approve any adequacy decisions, declined to give its approval at a meeting in April 2000. The issue will therefore need to be brought before the Article 31 Committee again at a later point.<sup>46</sup>

Regarding its substance, the Safe Harbor Principles seem relatively meaningless because there is still no effective independent enforcement. Self-regulatory Programs such as TRUSTe and BBBOnline cannot be considered effective enforcement from a European perspective.<sup>47</sup> Without effective independent enforcement the Safe Harbor cannot be seen as a viable long-term solution for the international privacy crisis.

Even if the Safe Harbor Principles could give guidance to non-European companies on a number of specific personal data collection practices online and offline, some of the

---

<sup>45</sup> See <<http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm>>.

<sup>46</sup> Art. 25(6) gives the EU Commission the power to take adequacy decisions only with the support of a qualified majority of the Member States in the Committee set up under the procedure of Article 31 of the Directive (Article 31 Committee). Such decisions are binding on the Member States.

<sup>47</sup> See *infra* Chapter II.C.4.c).i.

most controversial practices such as online profiling remain unaddressed by the Safe Harbor Principles.<sup>48</sup>

In the course of an earlier communication with the Department of Commerce Mogg specifically called into memory that the Safe Harbor discussions are not supposed to resolve nor prejudge the question of whether or when U.S. based Web sites may be subject to Member State or EU jurisdiction or applicable law issues. “All existing rules, principles, conventions and treaties relating to international conflicts of law continue to apply and are not prejudiced in any way by the Safe Harbor arrangement.”<sup>49</sup> Since this is still the case, one can seriously doubt that the Safe Harbor Agreement will prevent European consumers from bringing action against U.S. companies within their own legal systems.

Furthermore, only the personal data of European citizens processed by U.S. companies are subject to the Safe Harbor Principles. U.S. citizens are legally not covered by the Safe Harbor Principles. U.S. Businesses will certainly run into a serious public relations dilemma, once U.S. consumers find out that “legal aliens” are enjoying higher data protection standards.

Overall the Safe Harbor does not demonstrate any international consensus with long term viability. I will analyze other ways of finding such consensus in Part III of this thesis. As a political matter, however, the Safe Harbor Agreement seems important. It has the potential to stabilize trust in trade and investment. In addition, the Safe Harbor discussions helped to crystallize the main areas of disagreement between the two sides.

---

<sup>48</sup> Moreover, the Safe Harbor does not include the financial services sector, which is in the process of implementing regulations contained in the Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999, PL 106-102, Nov. 12, 1999, 113 Stat. 1338) passed by Congress in 1999.

<sup>49</sup> See Letter from John Mogg, *supra* note 40.

Mainly these areas of disagreement can be attributed to fundamentally distinct visions on democratic governance<sup>50</sup>, rather than to often-cited mere systemic differences in the approach to data protection rights (see Part II).<sup>51</sup>

---

<sup>50</sup> See J. Reidenberg, *supra* note 1.

<sup>51</sup> See Article 29 Working Party, Discussion Document: First Orientation on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy, Eur. Comm. Doc. DG XV D/5020/97 – WP 4, (Jun. 26, 1997) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp4en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp4en.htm)>.

## II. CLASHING PRIVACY REGIMES IN A WORLD OF SHARED PRIVACY PRINCIPLES

### A. INTRODUCTION

The Safe Harbor debate has shown that the social, political, and legal contexts in which privacy issues are addressed in the United States differ significantly from those in Europe.<sup>52</sup> A number of multilateral instruments<sup>53</sup> and academic scholarship<sup>54</sup> illustrate, though, that democracies converge on a basic set of principles for data protection. However, at a national level major divergences in the execution of these principles can be found - as the EU – U.S. controversy illustrates graphically.<sup>55</sup>

The convergence on basic principles can be attributed to historical factors.<sup>56</sup> Interest in the right of privacy increased in the 1960s and 1970s in Europe as well as in the U.S. with the advent of information technology (IT). The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information.<sup>57</sup>

---

<sup>52</sup> See FRED CATE, *PRIVACY IN THE INFORMATION AGE* 49 (1997).

<sup>53</sup> See, e.g., COE Convention, *supra* note 3; OECD Guidelines, *supra* note 4.

<sup>54</sup> See, e.g., F. CATE, *supra* note 52, at 97; Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, in *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE*, 102-05 (Phil E. Agre & Marc Rotenberg eds., 1997); J. Reidenberg, *supra* note 1.

<sup>55</sup> See J. Reidenberg, *supra* note 1.

<sup>56</sup> Colin Bennett described this convergence on international privacy principles concisely and attributed it together with international harmonization efforts to common features of information technology, an elite network of policy activists and European restrictions on transborder data flow. See J. COLIN BENNETT, *REGULATING PRIVACY DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES*, 220-50 (1992).

<sup>57</sup> In many countries, new constitutions reflect this right. See, e.g., EPIC, *PRIVACY & HUMAN RIGHTS, AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS* (1999). Available at: <<http://www.privacyinternational.org/survey/Overview.html#Heading6>>. The genesis of modern legislation in the field of data protection can be traced to the first data protection law in the world enacted

Two international instruments evolved in response to a great increase in transborder data flows and reflect international consensus on basic privacy principles. The Council of Europe's 1981 "Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data" and the Organization for Economic Cooperation and Development's "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" articulate specific rules covering the handling of electronic data. These two agreements have had a profound effect on the enactment of laws around the world<sup>58</sup> and served as the basis for the EU Directive. These international agreements helped to shape out a core set of fair information practice principles to assure the participation of citizens in the collection and use of their personal data. These principles revolve around four sets of standards: (1) data quality; (2) transparency or openness of processing; (3) treatment of particularly sensitive data, often defined as data about health, race, religious beliefs, and sexual life among other attributes; and (4) enforcement remedies and mechanisms.<sup>59</sup>

---

in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978).

<sup>58</sup> Over twenty countries have adopted the COE Convention and another six have signed it but have not yet adopted it into law. The OECD guidelines have been widely used in national legislation, even outside the OECD countries.

<sup>59</sup> See PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION, 5-6 (1996).

## **B. CONVERGENCE ON INTERNATIONALLY AGREED BASIC PRIVACY PRINCIPLES**

### **1. The U.S. National Information Infrastructure Privacy Principles**

In 1995 the Clinton administration created the Information Infrastructure Task Force.<sup>60</sup> This task force is divided into three committees and subcommittees, one of which - the Privacy Working Group of the Information Policy Committee- is responsible for addressing the privacy issues posed by the proliferation of electronic information networks.<sup>61</sup> This task force promulgated a set of principles illustrating also the U.S. acceptance of the mentioned internationally agreed basic privacy principles. The document by the working group titled "*Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (NII Principles)<sup>62</sup> reflects the U.S. government's current vision of information privacy.

The NII privacy principles are divided into three categories: (1) general principles for all NII participants, (2) principles of users of personal information (which the EU Directive refers to as "data controllers"), and (3) principles for individuals who provide personal information (data subjects). For the first category, the working group identified the Information Privacy Principle<sup>63</sup>, the Information Integrity Principle<sup>64</sup>, the Information Quality Principle<sup>65</sup> as the three guiding principles.<sup>66</sup> For the category of information users

---

<sup>60</sup> The task force, which includes representatives from most cabinet departments, is charged with articulating the administration's vision for the National and Global Information Infrastructures (NII and GII, respectively), and identifying and eliminating obstacles to their deployment.

<sup>61</sup> See F. CATE, *supra* note 52, at 92.

<sup>62</sup> Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, (Washington, 1995).

<sup>63</sup> Personal Information should be acquired, disclosed, and used only in ways that respect an individuals' privacy.

<sup>64</sup> Personal Information should not be improperly altered or destroyed.

<sup>65</sup> Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

<sup>66</sup> See F. CATE, *supra* note 52, at 92.

the working group identified five principles<sup>67</sup>: Acquisition Principle<sup>68</sup>, the Notice Principle<sup>69</sup>, the Protection Principle<sup>70</sup>, Fairness Principle<sup>71</sup> and the Education Principle.<sup>72</sup> These principles address the complete range of information activities – data collection, storage, use, and dissemination. In addition, they establish the foundation of any form of information privacy protection: Notice. The third category of principles includes the following three principles: Awareness Principle<sup>73</sup>, the Empowerment Principle<sup>74</sup> and the Redress Principle.<sup>75</sup> According to the commentary the principles are supposed to apply broadly, for example to all of the parties who collect information in a transaction, not just the party dealing directly with the consumer.<sup>76</sup>

These principles clearly demonstrate convergence with internationally agreed fair information principles as contained in the OECD guidelines. So how is it possible then

---

<sup>67</sup> Privacy Working Group, *supra* note 62, at II.A-D.

<sup>68</sup> Information users should: (1) Assess the impact on privacy in deciding whether or acquire, disclose, or use personal information. (2) Acquire and keep only information reasonably expected to support current or planned activities.

<sup>69</sup> Information users who collect personal information directly from the individual should provide adequate, relevant information about: (1) why they are collecting the information; (2) what the information is expected to be used for; (3) what steps will be taken to protect its confidentiality, integrity and quality; (4) the consequences of providing or withholding information; and (5) any rights of redress.

<sup>70</sup> Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.

<sup>71</sup> Information users should not use personal information in way that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.

<sup>72</sup> Information users should educate themselves and the public about how information privacy can be maintained.

<sup>73</sup> Individuals should obtain adequate, relevant information about: (1) why the information is being collecting; (2) what the information is expected to be used for; (3) what steps will be taken to protect its confidentiality, integrity and quality; (4) the consequences of providing or withholding information; and (5) any rights of redress. *See* Privacy Working Group, *supra* note 62, at III.A.

<sup>74</sup> Individuals should be able to safeguard their own privacy by having: (1) a means to obtain their personal information; (2) a means to correct their personal information that lacks sufficient quality to ensure fairness in its use; (3) the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions; and (4) the opportunity to remain anonymous when appropriate. *See* Privacy Working Group, *supra* note 62, at III.B.

<sup>75</sup> Individuals should, as appropriate, have a means of redress of harmed by an improper disclosure or use of personal information. *See* Privacy Working Group, *supra* note 62, at III.C.

<sup>76</sup> *See* F. CATE, *supra* note 52, at 93.

that there are information practices tolerated in the U.S. that seem to infringe various principles of international privacy agreements to which the U.S. is a signatory?

## 2. EU Principles

### a) *EU Principles Converging with Basic Principles*

In the 1998 working document “Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive”<sup>77</sup> the Article 29 Working Party, laid out what it considers as constituting “adequate” protection. In order to analyze whether a certain privacy regime meets European standards, the Working Party considers not only the content of rules applicable to personal data transferred to a third country, but also the system in place to ensure the effectiveness of such rules. Such laws have generally included additional procedural mechanisms, such as the establishment of supervisory authorities with monitoring and complaint investigation functions. These procedural aspects – that are largely absent in the U.S. privacy regimes - are reflected in the EU Directive by its provisions on liabilities, sanctions, remedies, supervisory authorities and notification.

Hence, the Working Party analysis of adequate protection comprises two basic elements: the content of the rules applicable and the means for ensuring their effective application. Thereby the Working Party seeks to arrive at a ‘core’ of data protection ‘content’ principles and ‘procedural/enforcement’ requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate.<sup>78</sup> It

---

<sup>77</sup> See Article 29 Working Party, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, (Jul. 1998)

<[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp12en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp12en.htm)>.

<sup>78</sup> See Article 29 Working Party, *supra* note 77, Ch.1.

derives this list of minimum requirements for privacy protection from the provisions of the Directive and other international data protection texts.<sup>79</sup>

According to the Working Party the basic principles to be included in a data protection are the following: (1) the Purpose Limitation Principle<sup>80</sup>, (2) the Data Quality and Proportionality Principle<sup>81</sup>, (3) the Transparency Principle<sup>82</sup>, (4) the Security Principle<sup>83</sup>, (5) the Rights of Access Principle, (5) the Rectification and Opposition Principle<sup>84</sup>, and (6) the Restrictions on Onward Transfers Principle.<sup>85</sup> Furthermore in some situations, additional principles relating to sensitive data<sup>86</sup>, direct marketing<sup>87</sup> and automated individual decision must apply.<sup>88</sup>

The Working party stressed that the existence of effective and dissuasive sanctions plays an important role in ensuring respect for rules, as of course can systems of direct

---

<sup>79</sup> See Article 29 Working Party, *supra* note 77, Ch.1.

<sup>80</sup> Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive.

<sup>81</sup> Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

<sup>82</sup> Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the Directive.

<sup>83</sup> Technical and organizational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

<sup>84</sup> The data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the Directive.

<sup>85</sup> Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive.

<sup>86</sup> Where 'sensitive' categories of data are involved (those listed in Article 8 of the Directive) additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

<sup>87</sup> Where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

<sup>88</sup> Where the purpose of the transfer is the taking of an automated decision (in the sense of Article 15 of the Directive) the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

verification by authorities, auditors, or independent data protection officials. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints. Finally, a data protection system must provide appropriate redress to the injured party where rules are not complied with. This is a key element, which must involve a system of independent adjudication or arbitration that allows compensation to be paid and sanctions imposed where appropriate.<sup>89</sup>

### **3. Fundamental Right Approach v. Market Oriented Approach**

Both the U.S. NII Principles and the core principles laid out by the Article 29 Working group create similar obligations and responsibilities. For example, collection of information should only be permitted for specific and specified purposes, the information should only be used in ways that are compatible with those purposes, information unnecessary to those purpose should not be collected, information should not be stored longer than is necessary for those purposes. Both systems recognize the importance of correcting inaccurate information, although, the U.S. principles would not guarantee individuals a right to access their personal information and would require correction only when the inaccuracy was so great as to compromise the fairness of the use of the data.<sup>90</sup> Both the EU Directive and the U.S. principles require that individuals be given notice whenever personal information is collected about them, and an opportunity to consent or withhold consent for certain uses of personal information. However, the importance given to substantive privacy rights differs greatly and produces significantly different levels of protection.

---

<sup>89</sup> See Article 29 Working Party, *supra* note 77.

Overall, both the EU and the U.S. privacy systems reflect numerous shared principles of information privacy despite the differences in which privacy issues are addressed. However, they protect those principles in different ways and to widely divergent degrees – as I will demonstrate in the following chapter. The ultimate question therefore becomes why do converging privacy principles translate so differently into legal rules in the EU as opposed to the U.S.

Before I will proceed with analyzing the differences of both regimes causing the current troubles, I will briefly introduce the two opposing patterns of perceiving of privacy that are usually referred to as the main source of the clash of privacy systems.

The EU Data Protection Directive's terms, and the process from which it resulted, reflect a commitment to privacy as a basic human right, on par with the rights of self-determination, freedom of thought, and freedom of expression.<sup>91</sup> This commitment to privacy as human right is also reflected in the efforts<sup>92</sup> to include data protection in the soon to come EU charter of fundamental rights.<sup>93</sup> The perception of privacy as a fundamental right and freedom empowers privacy concerns to override commercial concerns over regulatory costs. Any sort of cost benefit analysis as typically applied by U.S. regulators is therefore inappropriate under the EU approach. As Spiros Simitis, a former data protection commissioner in the German state of Hesse and chair of the Council of Europe's Data Protection Experts Committee, stated: "[w]hen we speak of data protection within the European Union, we speak of the necessity to respect the

---

<sup>90</sup> See F. CATE, *supra* note 52, at 97.

<sup>91</sup> See F. CATE, *supra* note 52, at 42.

<sup>92</sup> Article 29 Working Group, Recommendation 4/99 on the Inclusion of the Fundamental Right to Data Protection in the European Catalogue of Fundamental Rights  
<[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp26en.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp26en.htm)>.

<sup>93</sup> At its meeting on June 4, 1999 in Cologne, the European Council decided to draw up a charter of fundamental rights of the European Union.

fundamental rights of the 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.”<sup>94</sup>

By contrast, the U.S. that conceives of itself as a liberal state is committed to self-governance and individual rights. This political philosophy of nonintervention causes skepticism towards regulation of private relations, and translates in the privacy context into a narrow definition of personal information.<sup>95</sup> That narrow definition of personal data became an issue in the course of the Safe Harbor negotiations where the Europeans had to convince the Americans to expand the Safe Harbor Principles to cover also personal data of an “identifiable” individual – as covered under Article 2(a) of the Directive. Overall, this liberal theory approach urges a presumption in the U.S. that markets rather than law, should shape information privacy.

### **C. SUBSTANTIAL DIVERGENCE OF IMPLEMENTATION REGIMES**

#### **1. Background**

There are currently several models of privacy protection. Many countries around the world have enacted comprehensive data protection laws. These laws govern the collection, use and dissemination of personal information by both the public and private sectors. This is the model favored by the EU to ensure compliance with its data protection regime. In most of the countries with comprehensive data protection laws, there is also an official or agency that oversees enforcement of the act.

---

<sup>94</sup> S. Simitis cited in G. Shaffer, *supra* note 22, at 19.

<sup>95</sup> See J. Reidenberg, *supra* note 1.

Some countries such as the United States have avoided general data protection rules in favor of specific sectoral laws governing, for example, video rental records<sup>96</sup> and financial privacy.<sup>97</sup> In such cases, enforcement is sought through a range of mechanisms, such as oversight through industry oversight bodies or private litigation. Some countries – like the U.S., Japan or Singapore particularly promote privacy protection through various forms of self-regulation, in which companies and industry bodies establish codes of practice. However, codes of practice established through self-regulation lack adequacy and enforcement supervision.<sup>98</sup>

Other countries like New Zealand, Hong Kong and Australia have adopted hybrid models that I will discuss in further detail in Part III of this thesis.

## **2. The U.S. Privacy Regime**

In the United States, there is no explicit constitutional guarantee of a right to privacy. The Supreme Court, however, has interpreted many of the amendments, including the Bill of Rights, as providing some protection for various aspects of individual privacy against intrusive government activities.<sup>99</sup> That again reflects the U.S. preference for a government of limited powers. The Supreme Court's interpretation of constitutional protection for individual privacy is confused though. The scope of that protection is narrow, and the value of privacy interests is often limited when weighed against other,

---

<sup>96</sup> Video Privacy Protection Act of 1988, 18 U.S.C.A. § 2710 (the famous “Bork Law”).

<sup>97</sup> Right to Financial Privacy Act, PL 95-630.

<sup>98</sup> See EPIC, *supra* note 57, at 13.

<sup>99</sup> These include the First Amendment provisions for freedom of expression and association (U.S. Const. Amend. I; *see, e.g.*, NAACP v. Alabama, 357 U.S. 449 (1958)); the Third Amendment restriction on quartering soldiers in private homes, the Fourth Amendment prohibition on unreasonable searches and seizures, the due process clause and guarantee against self-incrimination in the Fifth Amendment, the Ninth and Tenth Amendment reservations of power in the people and the States, and the equal protection and due process clauses of the Fourteenth Amendment. None of these provisions refer to privacy explicitly, and the

more explicit constitutional rights. Moreover, it must be remembered that constitutional rights protect individuals only against state action.<sup>100</sup> As a result, any constitutional concept of “privacy” would apply only against the government and would at most require that the government refrain from taking actions, which impermissibly invade privacy. A constitutional privacy right would not require the government to take affirmative steps to protect individual privacy. Consequently, U.S. legislation provides citizens with significantly greater protection against the collection of personal information by the government than by the private sector – in fact, the private sector is virtually unregulated. The roots for such a strict distinction between the public and private can also be found in liberal political theory, according to which individuals need to be protected from collective control over their behavior.<sup>101</sup> This clearly requires stricter control of the public sector, whereas the private sector is left to the forces of the market. By contrast, in drafting the Data Protection Directive, the EU Commission was aware of the fact that neither clearly separating the private from the public sector nor limiting the protection of the data subjects to the former is possible. Patients in a private clinic are, as far as the use of their data is concerned, in the same situation as those treated in a hospital belonging to

---

circumstances in which privacy rights are implicated are as widely varied as the constitutional sources of those rights. *See* F. Cate, *supra* note 8, at 17-18.

<sup>100</sup> Only the Thirteenth Amendment, which prohibits slavery, applies to private parties. *See* *Clyatt v. United States*, 197 U.S. 207, 216-20 (1905). Although state action is usually found when the state acts toward a private person, the Supreme Court has also found state action when the state affords a legal right to one private party which impinges on the constitutional rights of another, *New York Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964), and in rare cases when a private party undertakes a traditionally public function, *Marsh v. Alabama*, 326 U.S. 501, 507-08 (1946), or when the activities of the state and a private entity are sufficiently intertwined to render the private parties’ activities public, *Evans v. Newton*, 382 U.S. 296, 299 (1966).

<sup>101</sup> *See* G. Shaffer, *supra* note 22, at 28, citing Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423 (1982).

the state. Employees are confronted by the same problems with respect to their data whether they are employed by a computer firm or by a tax authority.<sup>102</sup>

Most U.S. privacy laws reflect a predominance of public sector privacy regulation. The Privacy Act of 1974<sup>103</sup>, for example, protects records held by the U.S. Government agencies and requires agencies to apply basic “fair information practices.” However, effectiveness of this law is significantly weakened by administrative interpretations of a provision allowing for disclosure of personal information for a “routine use” compatible with the purpose for which the information was originally collected.<sup>104</sup> Laws like the Electronic Communications Privacy Act of 1986 (“ECPA”), which regulates the interception of private communications and access to and disclosure of stored electronic communications, also specifically forbids the federal government from snooping into online communications systems.<sup>105</sup> ECPA does not provide the same privacy protection to personal data collected by private entities.<sup>106</sup> In addition, a patchwork of federal laws covers some specific categories of personal information. These include financial records<sup>107</sup>, credit reports<sup>108</sup>, video rentals<sup>109</sup>, cable television<sup>110</sup>, educational records<sup>111</sup>, motor vehicle registrations<sup>112</sup>, and telephone records<sup>113</sup>.

---

<sup>102</sup> See S. Simitis, *supra* note 7, at 452.

<sup>103</sup> Privacy Act of 1974, 5 U.S.C.A. § 552a, PL 106-170.

<sup>104</sup> See EPIC, *supra* note 57, at 164.

<sup>105</sup> See, e.g., *Mc Veigh v. Cohen*, 983 F. Supp. 215 (D. D.C. 1998).

<sup>106</sup> See Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, STAN. TECH. L. REV 1 (1999)

<[http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_1/index.htm](http://stlr.stanford.edu/STLR/Articles/99_STLR_1/index.htm)>.

<sup>107</sup> Right to Financial Privacy Act, PL 95-630.

<sup>108</sup> Fair Credit Reporting Act, PL 91-508, amended by PL 104-208 (Sep. 30, 1996).

<sup>109</sup> Video Privacy Protection Act of 1988, PL 100-618, 1988 (“Bork law”).

<sup>110</sup> Cable Privacy Protection Act of 1984, PL 98-549.

<sup>111</sup> Family Educational Rights and Privacy Act of 1974, PL 93-380.

<sup>112</sup> Drivers Privacy Protection Act of 1994, PL 103-322.

<sup>113</sup> Telephone Consumers Protection Act of 1991, PL 102-243.

Still there are many privacy critical practices in the public realm that are virtually not regulated or regulated in a way that leaves many loopholes. For example, most U.S. state motor vehicle departments (DMV) sell, or otherwise disclose, license data to private-sector interests.<sup>114</sup> These data include people's names, addresses, Social Security numbers, and photographs. The State of Indiana, for example, sells driver's license data, along with motor vehicle registration records and other information, directly over the Internet.<sup>115</sup> Driver's license records and registration records cost \$5.00 a piece.<sup>116</sup> The typical economic efficiency approach to privacy regulation enables U.S. regulators to justify such practices along the following lines: The sale of driver's license data provides a revenue source that can help state agencies adopt streamlined information technology systems that are useful to the general public.<sup>117</sup> The opportunity to generate revenue through the disclosure of driver's license data provides an incentive for states to improve their telecommunications systems and make services available to the general public.<sup>118</sup>

In the U.S. the focus on government efficiency became particularly strong in the late 1970s. By then, concerns about the size, efficiency and the increase in the federal deficit made management a policy priority. This was reflected during the Reagan administration in the establishment of a number of executive bodies with an emphasis on management.<sup>119</sup>

---

<sup>114</sup> See *Travis v. Reno*, 163 F 3d 1000, 1002 (7<sup>th</sup> Cir. 1998).

<sup>115</sup> See Access Indiana Premium Services page <<http://www.accessindiana.com/premium/index.html>>.

<sup>116</sup> See *Carlson/Miller*, *supra* note 118, at 83. Even if the U.S. Congress passed the Driver's Privacy Protection Act (DPPA) in 1994, 18 U.S.C.A. § 2721(a)-(d), many practices that under European Data Protection regimes would be prohibited remain permissible. The DPPA allows disclosure of data to private firms "in the normal course of business" to verify or correct existing data. State motor vehicle departments are also allowed to disclose their data for bulk distribution of marketing surveys and solicitations if individuals have an opportunity to opt-out.

<sup>117</sup> The State of Wisconsin, for example, generates roughly \$8 million annually from the sale of driver's license data. See *Travis v. Reno*, 163 F 3d 1000, 1002 (7<sup>th</sup> Cir. 1998).

<sup>118</sup> See Steven C. Carlson & Ernest D. Miller, *Public Data and Personal Privacy*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 83, 97 (1999).

<sup>119</sup> Various bodies were created that advocated the use of computer and communication technology to enhance the efficiency of the federal government and particularly the use of computer matching as a

In recent years, there has been significant debate in the U.S. about the development of privacy laws covering the private sector. Critics of the U.S. approach of separating public from private maintain that private entities' activities need to be subject to similar controls because they can coerce or otherwise significantly influence individual behavior just as much as the government.<sup>120</sup> More than 100 bills on privacy protection were presented in the previous Congress, including laws such as the Online Privacy Protection Act of 1999, Internet Growth and Development Act of 1999, Electronic Rights for the 21st Century Act, Internet Privacy Protection Act of 1999, and the Social Security Online Privacy Protection Act of 1999.<sup>121</sup> However, the fact that only one proposal was approved as of October 1999 (Children's Online Protection Act, COPPA<sup>122</sup>) reflects the deeply rooted bias of the U.S. regulator toward distinguishing public from private and continuing economic efficiency thinking.

Reflecting this pattern, the U.S. regulator has traditionally preferred a system of industry self-regulation - the paragon of the market orientated privacy regulation - in order to deal with most privacy issues. In the 1997 report "Framework for Global Commerce" President Bill Clinton and Vice-President Albert Gore underscored the U.S. administration's preference for industry self-regulatory privacy regimes.<sup>123</sup> This form of

---

technique to detect fraud, waste and abuse. Representatives from these bodies were active in congressional policy making and extolled the benefits of computer matching, often without hard data in cost and benefit. See PRISCILLA M. REGAN, *LEGISLATING PRIVACY* 185 (1995).

<sup>120</sup> G. Shaffer, *supra* note 22, at 28. U.S. management theorist Peter Drucker wrote that in American society, the large corporation has become the "institution which sets the standard for the way of life and the mode of living of our citizens; which leads, molds and directs; which determines our perspectives on our own society; around which crystallize our social problems and to which we look for their solution." PETER FERDINAND DRUCKER, *THE CONCEPT OF THE CORPORATION* 6-7 (1946).

<sup>121</sup> See EPIC, *supra* note 57, at 165.

<sup>122</sup> 15 U.S.C.A. § 6501.

<sup>123</sup> However this general support for self-regulation was not without the reservation that if privacy concerns were not to be effectively provided by the industry through self-regulation and technology this policy would be re-evaluated, see William J. Clinton and Albert Gore, Jr., *A Framework For Global Electronic Commerce*, (July 1997) <<http://www.iitf.nist.gov/elecomm/ecommm.htm#no.1>>.

seeking privacy protection is, however, at odds with European regulatory tradition. Still, Article 26 (2) of the Directive allows data transfers out of the European Union, even to those countries that generally lack adequate protection, when there are other “adequate safeguards” in place. Therefore the Safe Harbor discussions revolved very much around the question of how self-regulation can be made a viable means to provide adequate privacy protection. Given that Europeans continued to view industry self-regulation very skeptically, U.S. Department of Commerce officials went over to defend U.S. practices, critiquing the European Union for its “top-down approach” of “privacy czars and bureaucrats” as antithetical to U.S. traditions of limited governmental intrusion into the private sector.<sup>124</sup>

The effectiveness of self-regulation has been particularly put into question regarding new privacy critical online business practices. The FTC has conducted a series of studies aimed to assess the effectiveness of self-regulation and privacy online. In June 1998 the Commission presented a report titled “Privacy Online” to Congress (“1998 Report”).<sup>125</sup> The FTC’s call for legislation with respect to children’s privacy rights supported by this study, led Congress to pass COPPA.<sup>126</sup> However, despite the alarming findings of the 1998 Report, the FTC did not recommend legislative action in the area of online privacy for consumers generally. Instead, it misconstrued in its 1999 progress report titled, “Self-Regulation and Online Privacy”<sup>127</sup> the findings of the “Georgetown Internet Privacy

---

<sup>124</sup> See E. Andrews, *supra* note 10, at A1 (quoting David Aaron, Under Secretary of Commerce); see also U.S. Government Working Group on Electronic Commerce, First Annual Report 18 (1998) (critiquing the EU’s “broad, centralized, top- down approach to privacy protection” that could disrupt “the free flow of information”).

<sup>125</sup> See FTC, *Privacy Online: A Report to Congress*, Jun. 1998, <<http://www.ftc.gov/reports/privacy3/toc.htm>>.

<sup>126</sup> PL 105-277.

<sup>127</sup> See FTC, *Self-Regulation and Online Privacy*, (July 1999) <<http://www.ftc.gov/os/1999/9907/privacy99.pdf>>.

Policy Survey” (GIPPS) issued in June 1999.<sup>128</sup> Bound by its own bias toward market-oriented regulation, the FTC ignored or misconstrued many of the survey’s findings and continued to promote industry self-regulation.<sup>129</sup> In fact, the survey clearly revealed that little or no progress has been made since the 1998 Report despite the FTC’s increased effort to convince the industry to introduce effective self-regulation.<sup>130</sup> Yet, the Commission concluded in its 1999 Report that legislation to address online privacy is not appropriate at this time.

### 3. The EU Privacy Regime

The tendency in Europe has historically been for data protection rules to be embodied in law, which has provided the possibility for non-compliance to be sanctioned and for individuals to be given a right to redress. The EU Directive follows the approach of already existing data protection laws of EU countries. National data protection laws of the EU Member States take a comprehensive omnibus approach and are often supplemented by sector specific laws and regulations that apply to specific types of processing activities for specific subject matters.<sup>131</sup>

The scope of the EU Directive is extremely broad when seen from a U.S. perspective. With only a few exceptions<sup>132</sup> it applies according to Article 3(1) of the Directive to all “processing” of “personal data.” The Directive covers “any operation or set of operations which is performed upon personal data, whether or not by automatic

---

<sup>128</sup> Mary J. Culnan, *Georgetown Internet Privacy Policy Survey (GIPPS)*, (June 1999) <<http://www.msb.edu/faculty/culnanm/gippshome.html>>

<sup>129</sup> See Ram Avrahami/The NAMED, Comments on GIPPS, <<http://www.msb.edu/faculty/culnanm/GIPPS/named.PDF>>.

<sup>130</sup> See also FTC Commissioner Sheila F. Anthony (dissenting with the majority view that legislation is not necessary), Statement on “Self-Regulation and Privacy Online,” FTC Report to Congress, <[http://www.ftc.gov/os/1999/9907/pt071399anthony.htm#N\\_3](http://www.ftc.gov/os/1999/9907/pt071399anthony.htm#N_3)>.

<sup>131</sup> F. CATE, *supra* note 52, 44.

means. According to Article 2(b) this includes 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 of data as “processing of data”.

“Personal data” is also used in a very broad sense. Article 2(a) defines it as 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.<sup>133</sup> This includes not only textual information but also photograph, audiovisual images, and sound recordings of an identified or identifiable person. The Directive is not limited to living natural persons.

Two categories of personal data are exempt from the scope of the Directive. According to Article 3(2) the Directive does not apply to the processing of data in the course of an activity falling outside the scope of Community law<sup>134</sup> and in any case of processing operations concerning public security, defense, State security<sup>135</sup> and the activities of the State in areas of criminal law.<sup>136</sup> Further it does not apply to processing of

---

<sup>132</sup> See Article 3 (2) of Directive 95/46/EC.

<sup>133</sup> The interpretation of when information relates to an “identifiable” person is not uniform amongst the EU Member States. These differences create important ambiguities in the application of data protection laws to critical online information such as IP addresses, *see* JOEL R. & PAUL M. SCHWARTZ, ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY – REGULATORY RESPONSES 124, (Dec. 1998) <<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.pdf>>.

<sup>134</sup> Such as those provided for by Titles VI and VII of the Treaty on European Union, <[http://europa.eu.int/eur-lex/en/treaties/dat/ec\\_cons\\_treaty\\_en.pdf](http://europa.eu.int/eur-lex/en/treaties/dat/ec_cons_treaty_en.pdf)> (consolidated version incorporating the changes made under the Treaty of Amsterdam, signed on Oct. 2, 1997). The treaty governs in its Title VI common rules on competition, taxation, and approximation of laws. Title VII governs economic and monetary policy. Both Titles reserve powers to the EU Member States.

<sup>135</sup> Including the economic well-being of the State when the processing operation relates to State security matters.

<sup>136</sup> Directive 95/46/EC, art. 13.

personal data that is performed by a “natural person in the course of a purely personal or household activity.”

Other than earlier Member States protection laws the Directive gives special attention to the private sector.<sup>137</sup> It applies to all organizations holding personal data in electronic or manual files and companies transferring data inside the EU. They are referred to as data “controllers” which means any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes.<sup>138</sup> Most organizations are required to register with national authorities.

Special consideration is afforded to “sensitive data.” The Directive provides greater scrutiny and protection to certain types of information dealing with race, religion, health, or political beliefs.<sup>139</sup>

National laws enacted in compliance with the Directive must provide that personal data may be used only for the legitimate purposes for which they were collected and kept in a form that does not permit identification of individuals longer than is necessary for that purpose.<sup>140</sup> Personal data may be processed only with the consent of the data subject.<sup>141</sup>

---

<sup>137</sup> This is in discrepancy with earlier national laws that applied more equivalently to both government and private handling of data.

<sup>138</sup> Directive 95/46/EC, art. 2(d).

<sup>139</sup> Directive 95/46/EC, art. 8.

<sup>140</sup> Directive 95/46/EC, art. 6(1).

<sup>141</sup> Directive 95/46/, Article 7.

## 4. Applying the Diverging Regimes: A Case Study About Online Profiling

### a) Introduction

The rapid change of online business practices challenges both the U.S. and EU privacy regimes. In order to illustrate how the divergence of both regimes plays out in practice, I will confront both regimes with the now very common practice of online profiling.

### b) What is Online Profiling

Online profiling is the practice of aggregating information about consumers' interests, gathered by tracking their movements online, and using the resulting consumer profiles to create targeted advertising on Web sites.<sup>142</sup> This and similar technologies allow the direct or indirect identification of individual Internet user. Advertising networks are using a technology called *cookie synchronization* to be able to effectively share cookies<sup>143</sup> and the information associated with them on the server side across multiple sites.<sup>144</sup> The effects of this practice is that if a single company gets to know a netuser's identity with the use of a cookie set, any of the other companies can easily discover the user's identity with a visit to their sites.<sup>145</sup>

---

<sup>142</sup> See, e.g., <<http://www.ftc.gov/os/1999/9909/FRN990915.htm>>.

<sup>143</sup> A cookie is a unique identifier that a web server places on a computer: a serial number for you Internet users that can be used to retrieve user records from their databases.

<sup>144</sup> See, e.g., <<http://www.guid.org>> or <<http://www.junkbusters.com/cookies.html>>.

<sup>145</sup> Another tool primarily used by the online advertising industry are so called "web bugs" (by the advertising industry also referred to as "clear gif") which is an inconspicuous graphic loaded on a Web page, usually from a different server than that used for the rest of the page. Web bugs are often invisible because they are extremely small. They are placed on a page to allow the source to record "hit" information about visitors to that page. This hit information is reported to the advertising networks that have a relationship with the site. Web bugs gather the IP-address of the computer that produced the hit. Web bugs also report the Universal Resource Locator (URL) of the page on which the web bug was placed, the URL for the Web bug graphic or image (which usually comes from a different server), the time the Web bug was viewed, the kind of browser the user is using and information about any cookie set by the web bug. The

The online advertising industry, especially companies that serve ads to Web sites that they do not operate themselves and tracking software developers that license their software to Web sites wishing to track their own visitors, made online profiling their business model. Network advertisers pool data about consumers who visit diverse sites in those networks, and sell or place online advertising based upon inferences about consumers drawn from the pooled data. In addition, there are companies specializing in measuring the popularity of particular online advertisements for advertisers.<sup>146</sup> The leaders in this industry are companies like *DoubleClick*<sup>147</sup>, *Abacus Direct* and *Netgravity*, *24/7 Media*, the *CMGi* group of companies (including *Engage Technologies*, *Accipiter*, that will include after mergers *AdForce*, *Flycast* and *I/Pro*), a variety of related businesses, such as the *Altavista* and *Lycos* portals/search engines and companies like *Excite*, *Matchlogic*, *Enliven*, *@Home* that are related by ownership with *AT&T* and *TCI*. Moreover, there is a chain of ownership linking the profiling companies into other kinds of online and offline businesses. Some of these companies offer customer profiles to other businesses for sale.<sup>148</sup> Those companies collect hundreds of pieces of information.<sup>149</sup> *Experian*, for example, has for years sold an “ailments” list identifying sufferers of

---

browser stores the information in a text file and this information is sent back to the particular server each time the browser retrieves a page from that server. See, e.g., Robert O’Harrow Jr., *Global Savvy Web Bug’s Impact on Privacy Draws Scrutiny Internet: Regulators are looking at stealth tool that tracks online users’ activities and soon may be used to identify them by name*, LOS ANGELES TIMES, Nov. 15, 1999.

<sup>146</sup> In July 1998 already, Vice President Gore asked the Department of Commerce to work with the Federal Trade Commission to encourage companies that build profiles about individuals by integrating information from a variety of database sources to implement effective self-regulatory mechanisms, see <<http://www.ntia.doc.gov/ntiahome/privacy/workshop/frn-workshop.htm>>.

<sup>147</sup> A 1998 study carried out for the European Commission contains an interesting case study on *DoubleClick* and the issue of data protection: Serge Gauthronet & Frédéric Nathan, ARETE, *On-line services and data protection and the protection of privacy*, 91, (December 1998) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/studies/serven.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf)>.

<sup>148</sup> See JUNKBUSTER, *Profiling - Comments to the Department of Commerce and Federal Trade Commission*, (Oct. 18, 1999) <<http://www.junkbusters.com/ht/en/profiling.html>>.

<sup>149</sup> See Saul Hansell, *Big Web Sites to Track Steps of Their Users*, N.Y. TIMES, (Aug 16, 1998) <<http://www.nytimes.com/library/tech/98/08/biztech/articles/16data.html>>.

conditions from hemorrhoids to depression, and *Acxiom* among others sell data including religious denomination.

In the course of the latest controversies over privacy critical online practices, industry representatives have conceded that names could actually be attached to the customer profiles.<sup>150</sup> The reassurance that names can only be attached to profiles if the customer provides this information, does not necessarily put customers at ease since it is still rather likely that one specific company that has everything about a person but his name can acquire the name by other means. Data trading or mergers between different companies as well as cookie sharing can help to fill data gaps on individuals, and thus finally make it possible to gain a complete personality profile of a person including name and address.<sup>151</sup>

Most Web sites' privacy policies are misleading with respect to the operations done by the entire network of sites using an ad placement service since they usually do not say anything about what these third-party advertising networks are doing through the very site. In addition, users don't have any control over what is being done with their data. Amazon's site, for example, declares that the company does not disclose information about individual customers or their purchases to outside parties. However, the policy statement also mentions that the company reserves the right to do so in the future.<sup>152</sup> Even if individual purchases are not to be reported to third parties it is still understandable that

---

<sup>150</sup> See FTC Online Profiling Workshop <<http://www.ntia.doc.gov/ntiahome/privacy/index.html>>. See also Jeri Clausing, *FTC Asked To Examine Data Profiling Practices*, N.Y. TIMES, (Nov. 9, 1999) <<http://www.nytimes.com/library/tech/99/11/cyber/capital/09capital.html>>.

<sup>151</sup> See, e.g., EPIC, *Privacy Advocates Call on FTC to Halt Online Profiling - Practice Threatens Consumer Privacy* (joint press release of privacy advocacy groups), (Nov. 5, 2000) <[http://www.epic.org/privacy/internet/profiling\\_press\\_release2.html](http://www.epic.org/privacy/internet/profiling_press_release2.html)>.

<sup>152</sup> Find Amazon's privacy policy at: <<http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html/002-3246953-8383405>>.

a consumer feels uncomfortable about his book purchases showing up on a list that might appear to be endorsed by his employer.<sup>153</sup>

In addition, Amazon.com's purchase circles showed up a new privacy related issue – namely the question of corporate confidentiality. Evidently the purchase circles have the potential to reveal a lot about a company's confidential corporate strategies to curious outsiders or competitors. Levi Strauss & Co. employees, for example, have been – according to the purchase circles – busily ordering the books “Strategic Brand Management,” “Building Strong Brands” and “Street Trends: How Today's Alternative Youth Cultures Are Creating Tomorrow's Mainstream Markets.” Asked about the view of Levi-Strauss about the purchase circles a spokesman of the company responded that officials would not comment on the Amazon lists because, “as you know, we're intently focused on revitalizing the brands here.”<sup>154</sup>

### ***c) Online Profiling and the U.S. Privacy Regime***

#### ***i. No Handle on Online Profiling Under U.S. Privacy Laws***

U.S. privacy laws do not offer any possibility to get control over these practices. In the Amazon case, for example, it is not possible to find a legal basis for a claim for following reasons: First, most privacy laws like the “Bork law”<sup>155</sup> governing video checkouts or library records do not apply when one has to deal with data of many individuals. And secondly, the privacy laws that might protect individuals in such cases

---

<sup>153</sup> Companies can now opt-out of the purchase circles by changing their purchase circles settings on a fairly hard to find page on the Amazon Web site:  
<[http://www.amazon.com/exec/obidos/subst/community/community-questions.html/002-3246953-8383405#no\\_participate](http://www.amazon.com/exec/obidos/subst/community/community-questions.html/002-3246953-8383405#no_participate)>.

<sup>154</sup> See David F. Gallagher, *Amazon Tries to Ease Privacy Worries*, N.Y. TIMES, (Aug. 30, 1999)  
<<http://www.nytimes.com/>>.

are not likely to apply to corporations. Considering trade secret law, a potential way to keep Amazon from inherently revealing corporate strategies to competitors, will also be likely to fail since Amazon is just summarizing what is being communicated to the outside world by company itself anyway.

As mentioned earlier, laws like the Electronic Communications Privacy Act (“ECPA”) do not provide the same privacy protection to personal data collected by private entities.<sup>156</sup> Some legal remedies could be available to children under the new Children’s Online Privacy Protection Act of 1998 (COPPA).<sup>157</sup> This Act requires Web sites that collect personal identifying information from children to provide actual notice to parents and obtain parental consent. Given that children are usually even less aware of the threats to their privacy the promulgation of COPPA seemed to be a really important legislative intervention. However, in order to spot privacy-critical online situations parents might often be well advised to rely on the usually more sophisticated computer literacy of their children. It remains to be seen whether this law will have any effect.

## ii. Self-regulatory Programs, Privacy Seals

The U.S. regulator traditionally followed a hands-off approach with respect to the Internet and promoted instead industry self-regulation.<sup>158</sup> Consequently, the question comes up, whether existing self-regulatory mechanisms can provide any means of protection in online profiling cases.

The Online Privacy Alliance, a coalition of industry groups, announced a set of online privacy guidelines, which apply to individually identifiable data collected online.

---

<sup>155</sup> Video Privacy Protection Act of 1988, PL 100-618, Nov. 5, 1988, 102 Stat. 3195.

<sup>156</sup> See Eric J. Sinrod & Barak D. Jolish, *supra* note 106, 1.

<sup>157</sup> 15 U.S.C.A. § 6501.

According to these guidelines OPA members agree to adopt a privacy policy that provides comprehensive notice of their information practices.<sup>159</sup> The notice includes disclosure of what information is being collected from consumers, how the information is used, whether the information will be disclosed to third parties, consumer choices regarding collection use and distribution of the information, data security measures, and steps taken to ensure data quality and access to information.

The major drawback of OPA is that it does not monitor the compliance of its members or provide sanctions for non-compliance, and as the above examples demonstrate, there have been plenty of cases of non-compliance. Thus, doubts about the efficacy of OPA are certainly justified.

Privacy seal programs such as TRUSTe<sup>160</sup> or BBBOnline have shown to be not very effective. TRUSTe has apparently proven to be very reluctant to take action against privacy violations.<sup>161</sup> For example, RealNetworks' privacy policy which is certified by TRUSTe did not, disclose the existence of the Globally Unique Identifier (GUID) until the news about RealJukebox privacy invasions were released and still does not reveal that email addresses are transmitted along with GUIDs to RealNetworks. Already before that, TRUSTe had refused to launch an investigation into an apparent privacy violation committed by Microsoft: In March 1999 Microsoft revealed that it used GUIDs to render documents created by Microsoft Office software and visitors to Microsoft operated Web sites personally identifiable.

---

<sup>158</sup> See, e.g., Clinton/Gore, Framework, *supra* note 123.

<sup>159</sup> Find guidelines at: <<http://www.privacyalliance.org/resources/ppguidelines.shtml>>.

<sup>160</sup> See <<http://www.truste.org>>.

<sup>161</sup> See, e.g., EPIC comments on NTIA and FTC Online Profiling Workshop <<http://www.ftc.gov/bcp/profiling/comments/shen.htm>>.

People frequently do not realize that such an option exists, and data is often being collected en masse without their informed consent.<sup>167</sup>

Overall, under the perspective that Web sites and online advertisers operate more and more on the premise of collecting as much information as possible from consumers, the failure of self-regulatory programs and seal programs does not really surprise. The market does currently not provide a real incentive for the industry to consider their privacy policies, except in those few cases where privacy practices of company grew into a major public relations debacle for the company. Bad publicity about privacy practices had for instance some repercussion in the Doubleclick affair that marked the first time that privacy-related problems dramatically affected a company's value on Wall Street. Doubleclick – a company that serves advertising banners to thousands of Web sites and keeps track of the users as they move between sites - has drawn fire from privacy groups since it announced merger plans with offline direct marketing firm Abacus Direct in June 1999. This merger has put together online profiles obtained from an estimated 850 million Internet advertisements per day and 88 million personally identifiable five-year catalog purchase histories.<sup>168</sup> In January 2000 the company said it would begin associating people's names and addresses with its tracking program. Privacy groups

---

<sup>167</sup> Additionally, even if consumers were to get the opportunity to consent to the various forms of processing of their personal data it has to be borne in mind that consent as a principle of data protection can easily be abused. First, users may have no real alternative except to consent when their permission is sought before data processing (access to Web site denied). Secondly, data subjects may be unable to make an informed choice due to inadequate information about planned processing. With respect to the current practice of posting privacy policies the latter is most likely to be the case since most sites' privacy policies are usually hidden at the very bottom of a Web page.

<sup>168</sup> See EPIC, joint press release, *supra* note 151.

vehemently criticized the plan, and EPIC filed a complaint with the Federal Trade Commission against Doubleclick.<sup>169</sup>

**d) *Online Profiling Leaves the EU Data Protection System Scrambling***

Like the U.S. privacy regime, the EU Directive has difficulties in accommodating new privacy critical phenomena. The above case of online profiling reveals the major flaws of the Directive. In Article 14, for example, the Directive contains specific provisions for marketing purposes. However, it does not expressly cover profiling, as the German Information and Communications Services Act (IuKDG) does for instance. The latter permits the creation of user profiles only “under the condition that pseudonyms are used”. In addition, once profiles are created that are retrievable under pseudonyms, these data are explicitly forbidden from being combined with data related to the bearer of the pseudonym (Article 2, § 4(4) IuKDG).<sup>170</sup>

However, online profiling is clearly an action processing personal data as protected by the Directive. Thus, it falls within the scope of the Directive as described in Article 3.<sup>171</sup>

Online profiling raises particularly many issues associated with the finality of data use as required by Article 6(1)(b) of the Directive. This for Americans probably most

---

<sup>169</sup> See, e.g., Chris Oakes, *DoubleClick Plan Falls Short*, WIREDNEWS, (Feb. 14, 2000) <<http://www.wired.com/news/business/0,1367,34337,00.html>>. In a Wallstreet Journal Article of March 2000, Doubleclick chairman and CEO O'Connor sought to use the specter of the high costs of Net privacy to defuse the controversy. He argued that if Web sites were not allowed to collect information about users, the Web would become a subscription-only medium. Kevin O'Connor, *The High Cost of Net Privacy*, THE WALL ST. J., Mar. 7, 2000, at A26.

<sup>170</sup> See REIDENBERG/SCHWARTZ, ON-LINE SERVICES, *supra* note 133, 96 (Dec. 1998).

<sup>171</sup> The Data profiler is *natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*. The data profiler therefore is the data controller in the sense of Article 2(d) of Directive 95/46/EC.

surprising principle<sup>172</sup> is the limitation on “secondary” use of data: Although data might be collected “for specified, explicit and legitimate purposes,” they may not be further processed in a way incompatible with those purposes.”<sup>173</sup> Most online profiling activities, however, enable the use of personal data for multiple purposes.

Profiling practices are also at odds with the principle that unnecessary personal information should not be collected.<sup>174</sup> The collection of clickstream data generated in the course of surfing from one Web site to another is already a technical standard on the Web, for instance.<sup>175</sup> Moreover, recording and use of user behavior raises issues in the context of the Directive’s provisions dealing with consent, data storage and purging.<sup>176</sup>

The characterization of individuals according to their online behavior brings another fundamental idea of data protection into play: the special consideration to be afforded to sensitive data. Behavior profiling of customers is emerging as a key factor for electronic commerce corporate strategy. Consequently, data profiling regularly approaches the realm of sensitive data that are subject to processing prohibitions under Article 8 of the Directive: Isolated pieces of personal information collected in the course of online service activities may not be “sensitive data”. They might be brought within the meaning of “sensitive data,” though, by the use of typical online profiling practices.<sup>177</sup> Yet, the Directive does neither provide solutions for the sensitive data implications of online profiling nor resolve the judgements that will have to be made concerning the scope of

---

<sup>172</sup> U.S. privacy law views secondary use without the consent of the subject as lawful where there are no restrictions by statute or in the contractual arrangement. *See* RICHARD C. TURKINGTON & ANITA L. ALLEN, *PRIVACY LAW, CASES AND MATERIALS* (1999), 315.

<sup>173</sup> Especially under French law, the use of personal information is strictly limited to the purposes declared at the time of collection, *see* REIDENBERG/SCHWARTZ, *supra* note 133, at 90.

<sup>174</sup> Article 6(1)(c) Directive 95/46.

<sup>175</sup> This information can even extend to how long an individual has looked at a given page on a particular Web site.

<sup>176</sup> Directive 95/46/EC, art. 6(1)(c), 7.

“identifiable” information. Furthermore it does not resolve the issues of consent of individuals for profiling.<sup>178</sup>

The EU Member States are still unsettled in their approach to online profiling. In light of the earlier mentioned divergences in perception of certain data protection issues among the Member States, the transposition of the European Directive into national law is unlikely to resolve for the Internet immediately.<sup>179</sup> There are still different perceptions among the Member States concerning the way of how to deal with the requirement of data minimization, the requirement that online interactions be anonymous to the greatest extent possible (German IuKDG), the scope of the definition for “identifiable” information, the form of consent in the context of processing and profiling sensitive data for online services.<sup>180</sup> It will thus mainly depend on the manner in which Member States will treat these issues if these practices will be deemed an unlawful processing of personal data.

## **5. Most Substantial Divergence on Protection of Secondary Use of Data, Sensitive Data and Enforcement**

As the online profiling case illustrates, one of the major differences between the U.S. and the EU approach to privacy protection is that U.S. privacy law does not recognize the principle of a restriction to secondary use of data. As mentioned above, it views secondary use without the consent of the subject as lawful where there are no restrictions by statute or in the contractual arrangement.<sup>181</sup> By contrast, under EU law it is a basic

---

<sup>177</sup> See REIDENBERG/SCHWARTZ, *supra* note 133, at 85.

<sup>178</sup> See REIDENBERG/SCHWARTZ, *supra* note 133, at 137.

<sup>179</sup> See REIDENBERG/SCHWARTZ, *supra* note 133, at 139.

<sup>180</sup> See REIDENBERG/SCHWARTZ, *supra* note 133, at 135.

<sup>181</sup> See TURKINGTON/ALLEN, *supra* note 172, 315.

principle that further transfers of the personal data by the recipient of the original data transfer are permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.<sup>182</sup>

The online profiling debate also showed that the two regimes diverge substantially in the realm of the protection for sensitive data. The EU Directive prohibits the collection or use of data identifying “racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion...or concerning health or sexual life,” and requires special government scrutiny of any data collection and processing activities applicable to such information.<sup>183</sup> By contrast, U.S. laws do not include any such provision and provide for no government supervisory authority or data protection register.

Most substantially the EU and the U.S. diverge on the issue of enforcement. Government oversight of the data processing activities of private parties and enforcement of the law when necessary is a key principle under European law. Under the Directive that oversight means registration of all data processors and collection and processing activities with the national data protection commissions.<sup>184</sup> The U.S.’ constitutional commitment to a government of limited powers, particularly when expression is involved, posed a substantial obstacle to the creation of such government privacy authority.<sup>185</sup> Reflecting the U.S. liberal regulatory approach of nonintervention, also the NII principles remain silent on the enforcement of privacy rights against data collectors and processors.

---

<sup>182</sup> See Article 29 Working Party, *Transfers of Personal Data to Third Countries*, *supra* note 77.

<sup>183</sup> Directive 95/46/EC art. 8.

<sup>184</sup> Directive 95/46/EC art. 18.

<sup>185</sup> See F. CATE, *supra* note 52, at 98.

## D. DIFFERENT GOVERNANCE CHOICES THE DRIVING FORCE BEHIND DIFFERENT PRIVACY REGIMES

### **1. U.S. Privacy Concepts Reflecting Governance Choices**

In the U.S. the first legal paradigm in the history of privacy emerged at the end of the nineteenth century. The emergence of a newly industrialized society required a greater quantity and quality of information than the pre-industrial society.<sup>186</sup> In 1890, Warren and Brandeis articulated a concept of privacy as the individual's "right to be left alone."<sup>187</sup> The authors noted that the changing society created the need for new rights stating that "political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."<sup>188</sup> In light of this argument privacy is often cast as an individual's desire for seclusion from the public realm. However, Reidenberg underscores succinctly that "[t]his (right to be left alone) conception of privacy implicitly articulates a vision of the individual's liberty in society, namely that the individual has the ability to withdraw and associate with others. This also shows that privacy rights define relationships among citizens."<sup>189</sup> A fair claim could be made that Warren & Brandeis had already something along these lines in mind when they argued that privacy was the most cherished of freedoms in a democracy and that this freedom should be reflected in the Constitution.<sup>190</sup>

In more recent years, U.S. scholars have defined various conceptions of privacy also reflecting governance choices. Alan Westin, for example, conceives of privacy as the

---

<sup>186</sup> Rob Reilly, *Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward*, 6 RICH. J.L. & TECH. 6, 3 (1999).

<sup>187</sup> Warren & Brandeis, *The Right to Privacy*, 4 HARV.L.REV. 193, 195 (1890).

<sup>188</sup> Warren & Brandeis, *supra* note 187, at 193.

<sup>189</sup> See J. Reidenberg, *supra* note 1.

desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behavior to others.<sup>191</sup> He specifically interprets privacy as necessary for political participation.<sup>192</sup> Incorporating this autonomy theory of privacy, this “right to control the disclosure of personal information to others” sets the framework for private social interaction as well as political interchange.<sup>193</sup>

Edward Bloustein defines privacy as an interest of the human personality. According to him privacy protects the inviolate personality, the individual’s independence, dignity and integrity.<sup>194</sup> This dignity conception “would broadly set the constitutional ground rules for an individual’s interactions with others.”<sup>195</sup> In addition, the civility theory sees privacy as protection for community boundaries of decency.<sup>196</sup> Civility presents privacy as key instrument of social governance.<sup>197</sup>

Bovenzi views privacy more flexibly as “a subjective matter, the bounds of which depend on social norms that can change.” He speculates that, “in a world that fosters the application of new technologies to unusual activities and transactions, the introduction of new concepts of privacy, adapted to protect new interests, may render the new forms of communication less intrusive and more acceptable.”<sup>198</sup> Similarly Deirdre Mulligan, Staff Counsel for the Center for Democratic Technology (CDT) conceives of privacy as a mechanism that will evolve to “keep pace with changes in technology ... [and suggests

---

<sup>190</sup> Warren & Brandeis, *supra* note 187, 193-95.

<sup>191</sup> See ALAN WESTIN, *PRIVACY AND FREEDOM*, 7 (1967).

<sup>192</sup> See ALAN WESTIN, *supra* note 191, at 14.

<sup>193</sup> See J. Reidenberg, *supra* note 1.

<sup>194</sup> See Edward Bloustein, *Privacy as an Aspect of Human Dignity*, 39 NYU L. REV. 971 (1964).

<sup>195</sup> See J. Reidenberg, *supra* note 1.

<sup>196</sup> See Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL.L.REV. 957 (1989) (arguing that privacy protects rules of civility but the expansion of mass media poses an important threat to the rules). See J. Reidenberg, *supra* note 1.

<sup>197</sup> See J. Reidenberg, *supra* note 1.

that] [t]his requires a periodic assessment of whether changes in technology pose new threats to privacy that must be addressed through changes in law.”<sup>199</sup> Their conceptions appear to view privacy through the various risks associated with a loss of privacy generated by technological change.<sup>200</sup> In fact, as information technologies spread and the reliance on them increases, the general perceived risk to privacy is rapidly growing. Indeed, at its roots the privacy debate is very much about the allocation of risks connected with new privacy critical practices.<sup>201</sup> However, both Bovenzi’s and Mulligan’s positions primarily reflect the U.S. liberal governance choice which urges skepticism towards proactive comprehensive regulation. This does not necessarily exclude the possibility of viewing privacy decisions also through the lens of risks associated with a loss of privacy since the decision whether the state should step to deal with certain risks reflects after all also different governance choices. This connection becomes particularly evident when looking at the underlying historical patterns of the European data protection model.

## **2. The Evolution of the European Privacy Paradigm and the Distinctly European Context**

European democracies typically approach information privacy from the perspective of social protection. Under this governance philosophy, public liberty derives from the community of individuals and law is the fundamental basis to pursue norms of social and

---

<sup>198</sup> Giorgio Bovenzi, *Liabilities of System Operators on the Internet*, 11 BERKELEY TECH.L.J, 1 (Spring 1996) <<http://www.law.berkeley.edu/journals/btlj/>>.

<sup>199</sup> Testimony Before the Subcomm. on Courts and Intellectual Property, House Judiciary Comm., U.S. House of Rep. (March 26, 1998) (testimony of Deirdre Mulligan, Staff Counsel, Center for Democracy & Technology).

<sup>200</sup> See PERRI 6, *THE FUTURE OF PRIVACY*, 39-45 (1998).

citizen protection.<sup>202</sup> In light of this European perception of governance the state is regarded as the as the “necessary player to frame the social community in which individuals develop, and information practices must serve individual identity.”<sup>203</sup> Reidenberg frames this - from a U.S. perspective peculiar - approach as follows: “Citizen autonomy effectively depends on a backdrop legal rights.”<sup>204</sup>

The European commitment to treat privacy as basic human right is a “new and in many ways revolutionary approach to privacy.”<sup>205</sup> The evolution of European data protection has to be seen in its historical distinctly European context. Flaherty puts it as follows: “[E]uropean data protection laws include the hidden agenda of discouraging a recurrence of the Nazi and Gestapo efforts to control the population, and so seek to prevent the reappearance of an oppressive bureaucracy that might use existing data for nefarious purposes. This concern is such a vital foundation of current legislation that it is rarely expressed in formal discussions. This helps to explain the general European preference for strict licensing systems of data protection... [T]hus European legislators have reflected a real fear of Big Brother based on common experience with the potential destructiveness of surveillance through record-keeping.”<sup>206</sup> The eagerness of former east block countries to adopt strict EU-style data protection laws also shows this pattern.

Seen from this perspective the creation of government authorities with sweeping powers to oversee data-related activities appears paradoxical. However, this approach is consistent with the distinctive European governance preference reflected in the laws and

---

<sup>201</sup> See general on risk perception and risk communication: Richard C. Rich et al., *The Challenge of Risk Communication in a Democratic Society*, HEALTH, SAFETY & ENVIRONMENT Vol. 10 No. 3, 189 (Summer 1999).

<sup>202</sup> J. Reidenberg, *supra* note 1.

<sup>203</sup> *Id.*

<sup>204</sup> *Id.*

<sup>205</sup> F. CATE, *supra* note 253, at 42.

legal structures of most European nations. As Cate notes: “[I]ntensive government entanglement with daily life is accepted and often valued... [U]nlike the in the United States – where the constitution gives citizens rights against the government, but imposes few affirmative obligations in the government and provides no rights against private parties- European governments are often the guarantors of citizen rights and entitlements.”<sup>207</sup> In fact, EU citizens trust government more than private sectors with personal information.<sup>208</sup> Accordingly, the Data Protection Directive shows an acceptance of considerable government involvement in communications and the flow of information.<sup>209</sup> Privacy protection in Europe is therefore an exclusive issue of law. The law seeks to fully execute the basic privacy principles and thus provides prophylactic protection through comprehensive rights and responsibilities.<sup>210</sup>

In other words the EU privacy regime and underlying privacy fundamental right approach reflects a historically deep-rooted individual governance choice as does the U.S. regime. These divergent governance choices also find expression in various rights that stand in close connection with privacy and information that differ substantially from each other. So is the constitutional guarantee of freedom of expression and freedom of press, in fact subject to less governmental restraint in the U.S. than in the EU.<sup>211</sup>

## **E. CONCLUSION**

The clash of both privacy systems – as reflected in the now almost two year lasting EU - U.S. controversy - demonstrated that the differences between the two systems

---

<sup>206</sup> DAVID H. FLAHERTY, *PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES*, 373-74 (1989).

<sup>207</sup> F. CATE, *supra* note 253, at 44.

<sup>208</sup> J. Reidenberg, *supra* note 1.

<sup>209</sup> *See* F. CATE, *supra* note 52, at 45.

<sup>210</sup> SWIRE/LITAN, *supra* note 15, at 22-31.

outweigh the similarities. It turned out, though, through a comparison of the U.S. NII principles and the core principles upon which the EU Directive is based, that there is substantial convergence on fundamental internationally agreed principles. However, as the discussion of the respective privacy regimes showed, there are largely different systems of implementation of these basic principles in place. The online profiling case illustrated that the scope of legal protection executing basic privacy principles is far narrower in U.S. than in Europe.

This divergence in execution of privacy principles derives from fundamentally distinct views of democratic governance of both societies.<sup>212</sup> The EU and the U.S. do not share the same traditions and views on the role of the state in protecting the rights of citizens and the ability of the market to assure the fair treatment of citizens. Reidenberg puts it as follows: “[D]ata privacy rules are often cast as a balance between two basic liberties: fundamental human rights on the one side and the free flow of information on the other side...[t]he treatment and interaction of these liberties will express a specific delineation between the state, civil society, and the citizen.”<sup>213</sup>

I have demonstrated that the different governance philosophies manifest themselves particularly in the large gap between approaches to enforcement and different national policies interpreting the mentioned basic principles quite differently. The NII Principles illustrate this pattern: The empowerment principle purports to recommend the creation of substantive rights.<sup>214</sup> However, the commentary to principles clarifies that the extent to which those rights are actually provided “depends on various factors, including the

---

<sup>211</sup> See F. CATE, *supra* note 253, at 44.

<sup>212</sup> See also J. Reidenberg, *supra* note 1.

<sup>213</sup> See *id.*

<sup>214</sup> See F. CATE, *supra* note 52, at 94.

seriousness of the consequences to the individual of using the personal information and any first amendment rights held by the information user.<sup>215</sup>

Overall, the divergence of implementation regimes is therefore not just due to differences in legal systems. It goes to the core norms of a democratic society's organization regarding choices about the role of state, market and citizens in society. The national differences are therefore more profound than the politics leading to the choice of policy instruments.<sup>216</sup> On the search for an approach to avoid future clashes this has to be borne in mind.

---

<sup>215</sup> Privacy Working Group, *supra* note 62, at ¶30.

<sup>216</sup> See J. Reidenberg, *supra* note 1.

### **III. AN APPROACH TO AVOID FUTURE CLASHES OF PRIVACY REGIMES IN A GLOBAL CONTEXT**

#### **A. INTRODUCTION**

The insight that national differences derive from different visions of governance and privacy rules reflect a nations approach to governance, implies that efforts to harmonize specific standards would create conflicts with the way any model incorporates a market-based philosophy or a rights-based philosophy of governance.<sup>217</sup> A harmonization of standards therefore seems inappropriate to bring about an internationally viable solution. The recently co-regulatory approach - the simultaneous application of multiple rules to a unique information processing activity - recently proposed by Reidenberg, seems more likely to enable a “peaceful co-existence” of privacy regimes.<sup>218</sup> The EU – U.S. controversy has prepared the ground for such a process. It needs to be defined who will start that process and move it forward towards the goal of peaceful co-existence.

In the following I will review the impact that the EU Directive had on internal policy debates and the role that internal policies could have on reconciling the clashing privacy regimes. Further, I will examine the role that international institutions will play in avoiding regulatory conflict.

---

<sup>217</sup> *See id.*

<sup>218</sup> *See id.*

## **B. THE IMPACT OF THE EU – U.S. CONTROVERSY ON INTERNAL PRIVACY DEBATES**

### **1. U.S. Policy Debate**

The battle over privacy standards is fought not just between the EU and the U.S. “It is a civil war as well, fought within the United States itself, with European law changing the balance of power on the fields where U.S. interest groups clash.”<sup>219</sup>

When the U.S. legislature began regulating certain privacy critical sectors and practices, each case was defined as balancing an individual interest in privacy versus a societal interest (e.g. protection of driver’s data v. revenue for streamlined information technology systems useful to the general public). As a consequence of that political constellation privacy advocates were for a long time placed on the defense bearing the burden of proving that a particular activity invaded privacy.<sup>220</sup>

In the course of the international controversy with EU, the U.S. domestic debate over privacy regulation has been altered. Businesses are now on the defense about their practices.<sup>221</sup> Hence they are now busily trying to divert demands for stricter U.S. regulation, and to counter negative publicity at the same time.<sup>222</sup> Privacy advocates on the other hand have found themselves empowered with the argument that abandoning the system of self-regulation is a necessity in light of the international friction and commercial practices.

---

<sup>219</sup> See G. Shaffer, *supra* note 22, at 4.

<sup>220</sup> As Congress debated these issues, the focus on the value of privacy faded, to be replaced by the concerns of those whose particular interests would be jeopardized by the protection of privacy interests. The importance of privacy did not really carry weight in the normal legislative process. See P. REGAN, *supra* note 119, Ch. 7 (1995).

<sup>221</sup> See G. Shaffer, *supra* note 22, at 56.

<sup>222</sup> See G. Shaffer, *supra* note 22, at 56.

a) *U.S. Privacy Advocates*

In harmony with the EU social protection approach to privacy, U.S. privacy advocates<sup>223</sup> believe that individuals must be able to control the commercial use of personal information about themselves. Accordingly, they tend to employ a fundamental rights approach to promote their concerns.<sup>224</sup> Privacy advocates play an important role in the U.S. internal debate. They are constantly voicing their position in ongoing negotiations over U.S. data privacy rules. Privacy and consumer advocates consider EU Member States and EU officials as their allies. They provided them with support to demand tougher U.S. privacy protection standards.<sup>225</sup> The international debate has provided them with arguments in their efforts to promote stronger – individual rights focussed - U.S. protections through lobbying legislatures and agencies, intervening before courts, and using media to keep business data privacy practices in the spotlight.<sup>226</sup> Thus, the rights centered approach of the EU finds its way into the U.S. internal debate also through privacy advocates.<sup>227</sup>

In line with the European rights-centered philosophy, they maintained that the United States also needs “a comprehensive approach to privacy protection,” not a fragmented one. In the context of the Safe Harbor negotiations, privacy advocates used the opportunity to pressure the U.S. Department of Commerce to make the principles

---

<sup>223</sup> See, e.g., Center for Democracy & Technology (CDT) <<http://www.cdt.org/>>; Computer Professionals for Social Responsibility (CPSR) <<http://www.cpsr.org/>>; The Electronic Frontier Foundation (EFF) <<http://www.eff.org/>>; Electronic Privacy Information Center (EPIC) <<http://www.epic.org/>>; Junkbusters <<http://www.junkbusters.com/>>; The NAMED <<http://www.named.org/>>; PrivacyExchange <<http://www.privacyexchange.org/>>; Privacy International <<http://www.privacy.org/pi/>>; Privacy Times <<http://www.privacytimes.com/>>.

<sup>224</sup> See, e.g., EPIC, *supra* note 57, at 4.

<sup>225</sup> See SWIRE & LITAN, *supra* note 15, at 170.

<sup>226</sup> See G. Shaffer, *supra* note 22, at 55.

<sup>227</sup> See *id.*, at 65.

more stringent. In his letter to Under Secretary Aaron<sup>228</sup>, Mark Silbergeld of the Consumers Union (speaking on behalf of most known consumer rights and privacy advocacy groups<sup>229</sup>) generally criticized the Department of Commerce for focusing on protecting U.S. businesses from EU privacy requirements instead of protecting U.S. consumers from business exploitation of private information. Silbergeld also pointed out that it is becoming increasingly clear that large industry mergers in the telecommunications and financial services sectors have made the sectoral approach increasingly obsolete.<sup>230</sup> In the context of self-regulatory programs such as OPA (Online Privacy Alliance<sup>231</sup>) or seal programs such as TRUSTe<sup>232</sup>, privacy advocates revealed several breaches of self-regulatory codes that did not lead to any sanctions for the particular company in breach of the rules – thereby affirming European suspicion about self-regulation. Accordingly, they noted that the information industry cannot realistically be expected to police itself on consumer privacy unless it is given a clear (legislative) incentive to do so.<sup>233</sup>

---

<sup>228</sup> Advocacy groups responded to the Department of Commerce's call for comments on its Safe Harbor Principles even though the Department directed its invitation only to "Industry Representatives."

<sup>229</sup> Center for Media Education, Consumer Federation of America, Consumers Union, Electronic Privacy Information Center, Junkbusters, The NAMED, Privacy International, Privacy Journal, Privacy Rights.

<sup>230</sup> Mark Silbergeld, Additional Preliminary Comments of Consumer and Privacy Groups on the Department of Commerce Safe Harbor Proposal, (Nov. 19, 1998) <<http://www.ita.doc.gov/ecom/comlabc.htm#silbergeld>>.

<sup>231</sup> The Online Privacy Alliance, a coalition of industry groups, promulgated online privacy guidelines, which apply to individually identifiable data collected online. According to these guidelines OPA members agree to adopt a privacy policy that provides comprehensive notice of their information practices. Guidelines available at: <<http://www.privacyalliance.org/resources/ppguidelines.shtml>>.

<sup>232</sup> See <<http://www.truste.org/>>.

<sup>233</sup> Even the Electronic Frontier Foundation (EFF), a group that co-founded the self-regulatory program "TRUSTe", now considers the program to be ineffective. EFF states that the time has come to move out of this awareness-raising mode through self-regulation into an action mode where real protection can only be achieved by means of legislation. Giving emphasis to this argument the EFF mentions that TRUSTe at the beginning was only successful because it came with real threat of government regulation and enforcement. "Only when companies were threatened with the specter of governmental regulation did they decide to embrace seal programs like TRUSTe and then BBBOnline." See EFF, EFF submits comments and a request to participate in the Federal Trade Commission's (FTC) Public Workshop on Online Profiling (Session III), (Oct. 18) <[http://www.eff.org/pub/Privacy/Profiling/19991020\\_req\\_to\\_prtc\\_com3.html](http://www.eff.org/pub/Privacy/Profiling/19991020_req_to_prtc_com3.html)>.

Some advocates called for the creation of a new U.S. privacy protection agency, analogous to the supervisory authorities mandated by the European Union. Other advocates, however, noted that this might be unrealistic in light of current attitudes in Congress. Seeking more government efficiency the U.S. Congress is currently considering closing existing agencies and is consequently unlikely to authorize funds for a new one.<sup>234</sup>

**b) U.S. Industry**

Given the difficulty of separating data collected within Europe from data collected elsewhere, the Directive effectively requires multinational businesses to conform all of their data processing activities to European law.<sup>235</sup> As mentioned earlier, multinational companies depend on unlimited information flows, especially in their interactions with third-party suppliers, customers, consultants, marketers, and other service providers, but also internally, within their complex networks of affiliates, joint ventures, and partnerships.<sup>236</sup>

Complying with the Directive's requirements was considered very costly and a loss of operational flexibility.<sup>237</sup> Particularly sectors like financial services (payment systems, investment banking, insurance, credit reports...), media, nonprofit organizations, Internet service providers, business and leisure travel, pharmaceuticals and direct marketing were very wary of a potential ban of data transfers from the EU. In fact, even businesses that

---

<sup>234</sup> On the other hand, a division within the FTC, the Department of Commerce, or another agency could be made responsible for overseeing and providing consumer support on all data privacy issues. *See* G. Shaffer, *supra* note 22, at 65. A bill introduced in March 2000 by two congressmen proposed the creation of a federal privacy commission that would decide what new regulations should apply to American companies. *See* Declan McCullagh, *Congress Wants Privacy Commission*, WIREDNEWS, (Mar. 15, 2000) <<http://www.wired.com/news/politics/0,1283,34968,00.html>>.

<sup>235</sup> *See* F. Cate, *supra* note 8, at 3.

<sup>236</sup> *See* G. Shaffer, *supra* note 22, at 39.

do not operate in Europe may run afoul of the Directive if they collect, process, or disseminate personal data via multinational networks.<sup>238</sup>

Consequently, U.S. businesses have vehemently objected to EU data privacy requirements. Driven by the fear that new data privacy legislation will significantly raise business compliance, transaction, operational, and opportunity costs<sup>239</sup>, businesses started to work independently and joined sector-specific and cross-sector business associations to lobby governmental representatives in order to leave data privacy to industry self-regulation.<sup>240</sup> In the case of the FTC and the Department of Commerce, for example, these lobbying efforts have generally been successful. Evidently, the fact that industry groups are given substantial influence in the political decision-making process also reflects the market-based governance choice of U.S. society. This certainly complicates the efforts for international co-operation.

However, large multinational businesses have started to cooperate through transnational networks such as the Transatlantic Business Dialogue, which links over one hundred multinational companies based in the United States and Europe.<sup>241</sup> More and more data privacy protection “principles” and “guidelines” have been promulgated as an attempt to regain consumer trust. A number of businesses and associations have adopted or are developing privacy codes, guidelines, and other measures. These self-regulatory

---

<sup>237</sup> SWIRE & LITAN, *supra* note 15, at 101.

<sup>238</sup> See F. Cate, *supra* note 8, at 3.

<sup>239</sup> These opportunity costs are reflected in a comparison of revenue generated from direct marketing in Europe and the United States. In 1997, direct marketing sales in the United States exceeded \$1.2 trillion dollars, almost ten times the amount of direct marketing sales in Europe, which totaled approximately \$125 billion dollars. The U.S. direct marketing industry reportedly grew by seven percent in 1998 and expects to maintain a 7% annual growth through 2002. The EU direct marketing industry and its growth prospects are minute in comparison. See G. Shaffer, *supra* note 22, at 18-19.

<sup>240</sup> They have even hired former FTC Commissioner Christine Varney as a consultant. Particularly the information technology industry dedicated enormous resources to influence government officials on data privacy issues. See G. Shaffer, *supra* note 22, at 70-72.

schemes were described as the “EU Directive’s bastard offshoots - the unplanned offspring of the EU Directives’ encounter with U.S. business.”<sup>242</sup>

c) *U.S. Policymakers*

Pressure from U.S. businesses has made this a high profile issue for the U.S. administration.<sup>243</sup> The specter of the EU Directive has pressured U.S. agencies, above all the U.S. Department of Commerce, to persuade U.S. businesses to make self-regulatory mechanisms a more meaningful alternative and supplement to government regulation.<sup>244</sup> This was important because otherwise the self-regulatory approach to privacy protection would have little credibility, which would hinder a compromise with the EU.<sup>245</sup>

Despite its general tendency toward market-based solutions, the U.S. administration meanwhile appears to be more divided over data privacy issues - particularly regarding the question whether comprehensive rules establishing a minimum standard could be a viable way. While the Department of Commerce continues to promote a clearly market-oriented approach, based on business “self-regulation,” some members of the Clinton Administration and some members of Congress, and the Federal Trade Commission (only for children’s privacy) have promoted introduction of baseline comprehensive legislation. Vice-President Gore, for example, has urged Congress to pass an “electronic bill of

---

<sup>241</sup> See <<http://www.tabd.org/>>.

<sup>242</sup> See G. Shaffer, *supra* note 22, at 73.

<sup>243</sup> See, e.g., Noah Shachtman, *EU Privacy Law is Awkward for US*, WIREDNEWS, (Oct. 23, 1998) <<http://www.wired.com/news/news/business/story/15779.html>>.

<sup>244</sup> The FTC noted in its July 1999 Report “*Self-Regulation and Privacy Online*” that online businesses are providing significantly more notice of their information practices than they were the year before. See FTC, *Self-Regulation and Privacy Online*, <<http://www.ftc.gov/os/1999/9907/privacy99.pdf>>.

<sup>245</sup> G. Shaffer, *supra* note 22, at 59.

rights” guaranteeing on-line privacy, in particular with respect to medical and financial records.<sup>246</sup>

*d) U.S. Public View*

Driven by numerous media reports about the pervasiveness of new technologies and about the EU - U.S. privacy crisis, there seems to be more awareness about risks to privacy in U.S. society today. Asked about which approach to take to deal with privacy issues the American public appears to approve with the typical market-oriented style of regulation. A survey released by Louis Harris & Associates and Dr. Alan Westin in June 1998 found that strong majorities of computer users and Net users agree with the Clinton Administration policy to allow industry and public-interest groups to develop effective privacy rules and practices for the Internet and to legislate only if the private sector fails to implement these policies. 79% of computer users, 80% of Net users, and 76% of Net users that buy products and services online support favor this approach. According to the survey a slight majority (51%) of Net users who buy products and services online believe that business incentives will be enough for companies to adopt good privacy standards and that legislation will not be needed. However, 47% of Net purchasers, 60% of Net users and 67% of computer users believe that only legislation and legal enforcement will make most businesses observe good privacy policies.<sup>247</sup>

---

<sup>246</sup> See U.S. Vice President Issues Proposals To Protect Online Privacy, Agence-France Presse, July 31, 1998. Gore’s electronic bill of rights includes the following: “(1) The right to choose whether one’s personal information is disclosed; (2) The right to know how, when and how much of that information is being used; (3) The right to see that information themselves; (4) The right to know if information is accurate and corrected if it is not.” U.S. Government Working Group on Electronic Commerce, First Annual Report 18 (1998). A number of other privacy bills are pending in Congress at the moment.

<sup>247</sup> Louis Harris & Associates, Inc. and Dr. Alan F. Westin, E-Commerce & Privacy: What Net Users Want, (June 1998) <<http://www.pandab.org/pabsurve.htm>>.

## 2. EU Internal Debate

### a) *Privacy Advocates*

There are also privacy and consumer advocates operating in Europe. Yet, reflecting the European citizens' acceptance of the government protecting social values such as privacy, advocacy groups are by far not as visible in the European policy arena as in the U.S.

The Transatlantic Consumer Dialogue (TACD), a group of consumer advocates on working on both sides of the Atlantic held its first meeting on electronic commerce in Brussels in April 1999, in the midst of U.S.-EU negotiations over the content of the Safe Harbor proposals. On that occasion the transatlantic consumer advocates passed a resolution urging the European Commission and the Member States to reject the Safe Harbor Proposal.<sup>248</sup>

Privacy International<sup>249</sup>, a London based privacy advocacy group consisting of computer professionals, academics, lawyers, journalists, jurists and human rights activists is monitoring companies' compliance with the EU Data Protection and the EU/U.S. negotiations on Safe Harbor. Privacy International that also works in association with the Electronic Privacy Information Center (EPIC), one of the most efficient privacy advocacy groups in the United States, announced that it will monitor data transmissions of major U.S. multinational companies and ensure that the EU Directive is enforced.<sup>250</sup> In addition,

---

<sup>248</sup> TACD, Safe Harbor Proposal and International Convention on Privacy Protection, (last visited Feb. 19, 2000) <<http://www.tacd.org/meeting2/electronic.html#safe>>.

<sup>249</sup> See <<http://www.privacyinternational.org/>>.

<sup>250</sup> See G. Shaffer, *supra* note 22, at 66. Privacy International specifically mentioned its monitoring of Electronic Data Systems, Ford, Hilton International, Microsoft, and United Airlines. It was reported that "the target companies say they are hurrying to meet Europe's privacy requirements." See Noah Shachtman, *supra* note 243.

Privacy International initiated the so-called “Big Brother Awards” awards given to the companies, government agencies and individuals that have most directly undercut privacy.<sup>251</sup>

**b) Businesses**

Also in Europe businesses felt handicapped by the requirements of the Directive. Not surprisingly it was in Britain, one of the EU Member States with one of the more liberal privacy laws on file before the Directive went into force, where first claims arose stating that the fundamental right concept would be too costly. The Directive was supposed to not only increase business transaction costs to obtain information, but also reduce businesses’ productivity when businesses fail to obtain that information, resulting in increased operating costs.<sup>252</sup> The British Bankers’ Association (BBA) claimed that simply compiling and safeguarding the required information and providing it to inquiring customers according to the requirements of the Directive will cost each major bank on average “in excess of 150 pounds” per customer request and that, in aggregate, the provision of such information to customers will cost each bank “millions” of British pounds.<sup>253</sup>

---

<sup>251</sup> The first “Big Brother Awards” were held in London in October 1998 followed by ceremonies in Washington D.C. and Vienna, Austria. At 2000 U.S. Big Brother awards held in April 2000 the advocacy group elected the U.S. Department of Commerce, Doubleclick, the Federal Aviation Administration, and TransUnion as the winners of the award.

<sup>252</sup> G. Shaffer, *supra* note 22, at 18.

<sup>253</sup> See FRED CATE, *supra* note 52, at 42-43 & FN 64 (1997) citing the “Home Office Consultation Paper on the Implementation of the EU Data Protection Directive--The British Bankers’ Association Response,” Annex I (costs). Marc Rotenberg, Director of Electronic Privacy Information Center (EPIC), countered this quite convincingly with arguing that credit reports as mandated by the Federal Credit Reporting Act are available in the United States for U.S. \$8. See G. Shaffer, *supra* note 22, FN 59, referring to a telephone interview with Marc Rotenberg.

The EU Commission appointed independent consultants to conduct a detailed cost-benefit study. This handbook study quite persuasively concludes that the financial impact would be minimal.<sup>254</sup>

### 3. Conclusion

The EU – U.S. privacy controversy has recently been used to establish the argument that foreign regulatory requirements for greater social protection can give rise to a ratcheting up of national standards.<sup>255</sup> This is unlike the main fears of globalization critics claiming that globalizing processes pressure governments to reduce social protection requirements. This brief review of internal policy debates shows that the international discussions have in fact had an impact on the U.S. domestic privacy debate. Yet, since the Safe Harbor Agreement does not really bring about any substantial changes it seems certainly premature to make this claim. The outcome of the privacy standards battle can still be quite the opposite from an improvement of national social protection standards in the U.S. In fact, what the Safe Harbor achieves is that Europeans are now giving way to industry self-regulation as providing adequate protection. From a European perspective this form of privacy regulation is very likely to be considered as a decline in protection standards.

However, the EU - U.S. long term deadlock over the Safe Harbor proposals has shown that structural divergences make international cooperation a necessity for effective data protection in a global information market. As mentioned earlier, the different privacy

---

<sup>254</sup> The purpose of this study was to examine the most cost-effective means for companies and other organizations to comply with the specific obligations resulting from the Directive. See EU Commission, Handbook on Cost Effective Compliance with Directive 95/46/EC “Mason Study” (August 1998) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/studies/handbook.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/handbook.pdf)>.

<sup>255</sup> See G. Shaffer, *supra* note 22.

regimes are creating enormous uncertainty especially with respect to their treatment of international data flows. International cooperation is therefore crucial with respect to both social protection and “consumer trust.”<sup>256</sup>

Given that the Safe Harbor Agreement does not provide any substantial improvements, the lack of privacy protection in the U.S. will stay a matter of controversy with Europe.<sup>257</sup> EU data protection officials will certainly continue to pressure U.S. domestic privacy policies and practices.

U.S. privacy advocates, however, will certainly not be able to push strong enough toward the necessary international co-ordination and to overcome structural divergences. Also merely bilateral agreements, such as the Safe Harbor Agreement, have obviously failed in reconciling international privacy regimes. Other players with international credibility and leverage need to step in order to minimize diverging views of regulation.

### **C. HOW TO REACH INTERNATIONAL CONSENSUS?**

#### **1. Structural Pitfalls**

Before thinking about a way to reconcile different privacy regimes one needs to recall the structural pitfalls that the different governance philosophies are likely to create.

While the U.S. market oriented approach appears to be efficient in many instances on economic grounds and could differentiate according to needs, economic efficiency will certainly not be what the Europeans will be concerned about on the search for

---

<sup>256</sup> Supporters of government privacy protection rules often argue that data protection laws would increase the level of electronic commerce. This argument is based on the idea that privacy rules can improve consumer confidence. Indeed polls show that many consumers believe their privacy at risk when they do business on the Internet, which leads to less commerce than would otherwise exist. Several studies have shown that privacy concerns are the major reasons for consumer reluctance to get involved in online

international consensus. Rather Europeans would be likely to point out that the U.S. liberal market approach would have clear implications regarding self-governance and democratic participation. Poor privacy standards in cyberspace, for example, raise two threats to this promise: first, by undercutting the development and maintenance of an individual's capacity for self-governance; and second, by discouraging participation in deliberative democracy.<sup>258</sup> A too liberal approach with respect to online interactions, would have a negative impact on individual self-determination by deterring individuals from engaging in the necessary thinking out loud and deliberation with others upon which choice-making depends.<sup>259</sup>

As described earlier, the EU fundamental rights approach raises the value placed upon protecting privacy as social value. As such it allows sweeping regulation - as contained in the Directive - and considerable costs imposed on individuals, private sector institutions, and governments. The tone of prescriptive and wordy regulation feeds the perception of many Americans that the EU model of data protection is an alien form of heavy handed regulation.<sup>260</sup> Characterizing privacy as a human right also increases the likelihood that such regulation will be upheld against challenges based on other rights offended by that regulation. Indeed, the fundamental rights approach gives "rights" an infinite value, eliminating the possibility of any cost-benefit analysis involving competing values. These values may include commercial property interests, efficiency concerns, the availability of low-cost goods and services, freedom of expression,

---

activities. The AT&T study "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy" found that only 13% of those in the study were either "not very" or "not at all" concerned about privacy.

<sup>257</sup> See SWIRE/LITAN, *supra* note 15.

<sup>258</sup> Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999).

<sup>259</sup> P. Schwartz, *supra* note 258, at 1647-67.

protection against crime, and other matters for legislatures, regulators, courts, and markets to take into account. The non-negotiability of rights both reduces efficiency and raises equity concerns. Efficiency is reduced because privacy interests are not balanced against other societal concerns, including access to low-cost goods.<sup>261</sup>

Therefore - as the Safe Harbor deadlock illustrated - this approach decreases the room for compromise when reconciling European privacy law with that of other nations. Realistically, U.S. regulators will not leave economic efficiency thinking in favor of the fundamental rights approach. Rather they will continue being open to claims that data protection laws would strongly interfere with the operation of the free market in a thriving new economy. Data protection laws would force organizations to alter their behavior, large transition costs would follow and experts would have to be hired.<sup>262</sup>

## 2. Promising Alternatives

In the context of the EU – U.S. deadlock, interesting alternative solutions to both systems have crystallized.<sup>263</sup> The U.S. government has so far ruled out omnibus data protection legislation. At the same time the private sector has failed to take the opportunity to deliver an acceptable package of enforceable principles – a task that was always realistically only achievable in a few well-organized sectors.<sup>264</sup> Thus, a privacy law that positively embraced self-regulatory initiatives in those sectors, while providing a

---

<sup>260</sup> Nigel Waters, *Re-Thinking Information Privacy - A Third Way in Data Protection?*, in Proceedings of XXIst International Conference of Privacy and Personal Data Protection Commissioners, 2 (Sep. 1999) <<http://www.pco.org.hk/conproceed.html#top>>.

<sup>261</sup> G. Shaffer, *supra* note 22, at 19-20.

<sup>262</sup> Mandatory rules are said to reduce electronic commerce in situations characterized by new business models, rapid innovation, products dependent on intensive use of personal data information, and an important role for new companies. For example, data protection would also reduce Internet marketing. *See* SWIRE/LITAN, *supra* note 15, at 77-78.

<sup>263</sup> *See* N. Waters, *supra* note 260.

<sup>264</sup> *Id.*, at 9.

default statutory scheme for everyone else, might be a viable alternative - particularly if the differences between this approach and the traditional European legislative model are emphasized.<sup>265</sup>

There are now some useful models, which combine the best of the European experience “without its bureaucratic overtones.”<sup>266</sup> Some privacy specialists pointed out that a healthy skepticism about the limits, and pitfalls, of state regulation can be combined with an acknowledgement that private sector is incapable of delivering self-regulation without the stimulus of legal requirements.<sup>267</sup> With signing the tentative Safe Harbor agreement the EU has signaled the possibility of adequacy being delivered without legislation. Still it is clear that a legislative framework will avoid the complexities of assessing adequacy on a case by case or sectoral basis.

The New Zealand, Hong Kong laws and the draft Australian legislation are examples for such an alternative solution. Those laws feature:

- Statutory requirements of compliance with data protection principles.
- Development of principles which, while true to the common international standards, have been written collaboratively with user representatives and which contain practical exemptions and exceptions.
- Provisions for sectoral codes of practice which cannot only vary the principles, but also provide for sectoral complaint handling and enforcement mechanisms as the primary compliance machinery.

---

<sup>265</sup> See *id.*, at 11.

<sup>266</sup> *Id.*, at 9.

<sup>267</sup> See Raab, Bennett, Gellman and Waters: Final Report: Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of data, Sep. 1998, <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/studies/adequat.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/adequat.pdf)>.

- Default complaints and enforcement machinery for those sectors which do not choose to develop a code of practice, or which adopt a code that only varies the principles and does not establish compliance machinery.
- Provisions for appeals in certain circumstances from decisions of code compliance bodies, to provide a uniform quality control mechanism for interpretation of the principles.
- Avoidance of any generic registration or licensing requirement.<sup>268</sup>

Such a model provides a central role, if desired, for industry “self-regulation.” In fact, this form of self-regulation is better labeled as co-regulation of government and industry.<sup>269</sup>

Since these newer laws also make an attempt to deal with issues such as anonymity and use of government identifiers, advancing them beyond the current EU model<sup>270</sup>, the EU is expected to assess laws such as those in place in New Zealand and Hong Kong as “adequate” for the purposes of data transfers under the Directive.<sup>271</sup> As a consequence the international acceptability of such an approach would rise. Thus, the Asia-Pacific data protection model may turn out to be a viable alternative to overcome the structural pitfalls caused by diverging governance philosophies that caused the EU and the U.S. privacy crisis.

---

<sup>268</sup> N. Waters, *supra* note 260, at 10.

<sup>269</sup> *Id.*, at 11.

<sup>270</sup> *Id.*, at 11.

<sup>271</sup> In light of the Safe Harbor Agreement, it will be difficult for the EU to reject as inadequate comprehensive laws incorporating faithful versions of the OECD Principles and detailed compliance and enforcement mechanisms, even if they do not meet 100% of the detailed requirements still being promoted by the Article 29 Working Party.

### **3. Intergovernmental Players and Technical Standard Bodies Can Push Forwards**

#### ***a) Introduction***

Particularly the decentralized data processing activities on the Internet have shown the need for an international, co-operative approach. Reidenberg points out succinctly that successful co-regulation could facilitate flows of personal information and assure data protection at the same time. This can only be achieved through international co-operation.<sup>272</sup> Intergovernmental institutions will become key players as they can help minimizing conflicts of differing governance and accompanying information privacy norms.<sup>273</sup> In addition - at least in an online context - technical infrastructure can play a key role in alleviating the disjunction between governance choices and privacy norms.<sup>274</sup>

#### ***b) OECD/Council of Europe***

At the beginning of the 1980s the OECD's "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" (1980)<sup>275</sup> and Council of Europe's "Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data" (1981)<sup>276</sup> were promulgated in response to the increase in transnational data flows.<sup>277</sup> These agreements had a profound effect on the enactment of laws around the world.

There has been general agreement to date that the principles in the OECD Guidelines of 1980 are still an appropriate and suitable foundation for data protection laws, although

---

<sup>272</sup> J. Reidenberg, *supra* note 1.

<sup>273</sup> *Id.*

<sup>274</sup> *Id.*

<sup>275</sup> OECD, *supra* note 4.

<sup>276</sup> COE, *supra* note 3.

there is a lot of room for differences of opinion about how these principles translate into rules. Both the OECD and the COE have re-awakened to the need for enhanced international co-operation in light of new intrusive practices and an ever-higher degree of transborder information processing activities.

The OECD itself has only recently re-affirmed the relevance of the 1980 Principles<sup>278</sup> reasserting itself in the business of data protection, particularly in the context of electronic commerce.<sup>279</sup> Given that the OECD guidelines apply to all sectors the OECD clearly attempts to examine in data privacy in a cross-sectoral manner. However, the focus remains on the economic perspective of data protection, putting “users” and “consumers” at the center.<sup>280</sup> Since the OECD draws on the market oriented model of privacy protection the U.S. will be likely to support such efforts. However - as Reidenberg points out - to the extent that countries following the social protective approach can influence OECD efforts, this might help to reduce conflicts and divergences.<sup>281</sup>

By contrast, the Council of Europe approaches the issue of international co-ordination from a citizen’s rights perspective. In February 1999 the Council of Europe adopted the “Guidelines for the protection of individuals with regards to the collection and processing of personal data on the information highway, which may be incorporated

---

<sup>277</sup> See J. COLIN BENNETT (discussing the political background of both agreements), *supra* note 52, at 130-40.

<sup>278</sup> Most recently at the OECD Ministerial Conference in Ottawa, Canada, October 1998 - Ministerial Declaration On The Protection Of Privacy On Global Networks, OECD Doc. DSTI/ICCP/REG(98)10 Final (Dec. 1998).

<sup>279</sup> See, e.g., OECD, PRIVACY PROTECTION IN A GLOBAL NETWORKED SOCIETY: AN OECD INTERNATIONAL WORKSHOP WITH THE SUPPORT OF THE BUSINESS ADVISORY COMMITTEE, VOL. VI NO. 58 (1998), <<http://www.oecd.org/dst/sti/it/secur/prod/reg98-5final.pdf>>.

<sup>280</sup> J. Reidenberg, *supra* note 1.

<sup>281</sup> See *id.*

in or annexed to Codes of Conduct.” These Internet guidelines<sup>282</sup> follow the European social protection model of data protection.<sup>283</sup> The major drawback of having the COE as an institutional driver for international co-operation is its comparatively small number of signatory countries. Most notably and certainly not by surprise the U.S. is not a member country of the Convention.

*c) WTO*

The WTO will certainly become involved in the privacy protection debate and “will force these issues from the organization’s historical commitment to trade liberalization and growth of economic market and constraints on state behavior.”<sup>284</sup> In fact, the services provisions of the WTO accords prohibit signatories from imposing restrictions on transborder data flows.<sup>285</sup> Consequently, the WTO will have jurisdiction to hear complaints against any national restraint on transborder data flows.<sup>286</sup>

In the light of the tone that sometimes dominated the EU – U.S. Safe Harbor discussions, the WTO might well get the impression that data protection argument is in fact used to cover an underlying trade issue. After all, EU chief negotiator Mogg mentioned the risk of a trade war in the course of the Safe Harbor negotiations.<sup>287</sup> Indeed,

---

<sup>282</sup> COE, Recommendation No.R(99) of the Comm. of Ministers, Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways, (Feb. 23, 1999) <<http://www.coe.fr/DataProtection/elignes.htm>>.

<sup>283</sup> The Council of Europe specifically sought to develop these guidelines in conjunction with European Commission.

<sup>284</sup> See J. Reidenberg, *supra* note 1.

<sup>285</sup> See Art. XIV(c)(ii) FINAL ACT EMBODYING THE RESULTS OF THE URUGUAY ROUND OF THE MULTILATERAL TRADE NEGOTIATIONS: AGREEMENT ESTABLISHING THE WORLD TRADE ORGANIZATION, <<http://www.wto.org/wto/eol/e/pdf/04-wto.pdf>>.

<sup>286</sup> In fact, the European Commission has requested consideration of data privacy issues by the Council for Trade and Services. See Mario Monti, Closing Address at the Rome Symposium: The Internet and Privacy: what regulation, (May 1998) <[http://europa.eu.int/comm/internal\\_market/en/speeches/rome0598.htm](http://europa.eu.int/comm/internal_market/en/speeches/rome0598.htm)>.

<sup>287</sup> See Declan McCullagh, *Safe Harbor Swimming in Circles*, WIREDNEWS, (Apr. 29, 1999) <<http://www.wired.com/news/news/politics/story/19414.html>>. The European Union delayed enforcing the

it is certainly not far-fetched to say that the EU would have a clear incentive to protect its own personal information processing industries that are already equipped to deal with the EU Directive's requirements since they had to comply with strict Member States' data protection laws already earlier.

Clearly, the WTO would follow liberal market perceptions of privacy. In light of this inherent bias of the WTO toward liberal market norms, it would be interesting to see whether a WTO panel would - in case of a complaint - approve with the EU's typical but not uncontested<sup>288</sup> "consumer trust argument" claiming that data protection laws are increasing the level of electronic commerce.<sup>289</sup>

#### *d) Technical Standard Bodies Enabling Harmonization in an Online Context*

The technical capabilities of new systems have critical ramifications for data protection.<sup>290</sup> For example, the results of the reforms of the Internet domain name systems may make localization of users and servers easy or impossible. Organizations such as the World Wide Web Consortium (W3C)<sup>291</sup>, the Internet Society<sup>292</sup>, ICANN<sup>293</sup> and the Internet Engineering Task Force (IETF)<sup>294</sup> are each forming data protection policies.

---

EU Directive's provisions on third-country transfers while negotiations take place. See G. Shaffer, *supra* note 22, at 44-45.

<sup>288</sup> See SWIRE/LITAN, *supra* note 15, at 81-82.

<sup>289</sup> In fact, polls show that many consumers believe their privacy at risk when they do business on the Internet, which leads to less commerce than would otherwise exist. The AT&T study "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy" found, for example, that only 13% of those in the study were either "not very" or not at all concerned about privacy. A 1998 Business Week poll showed that 61 percent of non-Internet users cite privacy as a key reason for nonuse. See "Online Insecurity," Business Week, March 16, 1998, 102. A 1997 study conducted by the Boston Consulting group for the privacy seal-program TRUSTe, estimated that electronic commerce would double over \$12 billion in 2000 if privacy programs were widely adopted by commercial Web sites. TRUSTe Internet Privacy Study, "Summary of Market Survey Results" (1997), 20. See <<http://www.truste.org>>.

<sup>290</sup> See J. Reidenberg, *supra* note 1.

<sup>291</sup> W3C, *About the World Wide Web Consortium* <<http://www.w3.org/Consortium/>>.

<sup>292</sup> Internet Society Mission Statement <<http://www.isoc.org/isoc/mission/>>.

<sup>293</sup> See <<http://www.icann.org>>.

<sup>294</sup> See <<http://www.ietf.org>>.

Thus, technical standard bodies are creating technical rules that embed policies for the international flow of personal information. Though primarily confined to an online context, these policies can lead to international harmonization since they usually disregard any national privacy preferences. However, these technical bodies focus on promulgating technical standards for market adoption, they are bound to view privacy from a liberal governance rather than a social protection perspective.<sup>295</sup> In this context one needs to note that ICANN has recently been heavily criticized for promulgating far-reaching policies with effects for every Internet user, without following principles of democratic participation and transparency.<sup>296</sup> In light of this legitimacy debate it remains to be seen whether the public will on the long run accept policy decisions of technical standard bodies without having a fair chance of participation.

#### **4. International Harmonization Through Technical Codes**

Decisions about standards are blending technical issues with policy choices. Technical standards offer the opportunity to implement fair information practices in any information transfer and – as Lessig points out - technical codes are self-enforcing.<sup>297</sup> Accordingly, many regard technology as the currently most efficient tool to provide privacy in an online context. Lessig refers to technical codes as regulatory codes and argues that technical codes make social choices.<sup>298</sup>

---

<sup>295</sup> See J. Reidenberg, *supra* note 1.

<sup>296</sup> See, e.g., Jeri Clausing, *Internet Board Opens Chile Meeting Amid Protests*, N.Y. TIMES, (Aug. 24, 1999) <[www.nyt.com](http://www.nyt.com)>.

<sup>297</sup> Larry Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 898 (1996).

<sup>298</sup> LARRY LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

The example of W3C's "Platform for Privacy Preferences" (P3P)<sup>299</sup> underscores this point. Interestingly, the debate surrounding this software tool showed that the possibility to make social choices prepares just another setting for the same controversy that underlies the EU – U.S. privacy crisis.

P3P conceives of privacy and data protection as something to be agreed between the Internet user, whose data are collected, and the Web site that collects the data.<sup>300</sup> The idea behind P3P is that the user consents to the collection of his personal data by a site, provided that the site's declared privacy practices, such as the purposes for which data are collected and whether or not data are used for secondary purposes or passed on to third parties, satisfy the user's requirements.<sup>301</sup> The so-called Open Profiling Standard (OPS) is intended to provide for secure transmission of a standard profile of personal data.

The social choice dimension becomes clearer looking at the decisions the World Wide Web Consortium took when it sought to develop a single vocabulary through which a user's preferences and the site's practices are articulated. However, in that context the Article 29 Working Party criticized that given the intentions that P3P be applicable worldwide, the P3P vocabulary was not developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalize lower

---

<sup>299</sup> See <<http://www.w3.org/P3P/Overview.html>>.

<sup>300</sup> See Joel Reidenberg (discussing the P3P and the W3C initiatives), *The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection*, LEX ELECTRONICA III: 2, (Nov. 1997) <<http://www.lex-electronica.org>>.

<sup>301</sup> Technically P3P functions by means of user agents that allow users to be informed of site practices (in both machine- and human-readable formats) and that automatically make privacy decisions based on these practices when appropriate. Consequently users need not read the privacy policies at every site they visit.

common standards.<sup>302</sup> Not surprisingly, the Working Party stressed that P3P must be applied within the context of a framework of enforceable data protection rules<sup>303</sup>, which provide a minimum and non-negotiable level of privacy protection for all individuals.<sup>304</sup> Yet, W3C certainly furthered idea of international harmonization by disregarding the possibility of adapting the P3P privacy vocabulary to the needs and regulatory context of specific geographic regions.

Depending on users' response to P3P, it might prove to serve as a tool capable of changing the so-called information asymmetry<sup>305</sup> between the company and the customer. Thus, P3P might help disciplining the industry since the more users incorporate it into their browsers the less traffic Web sites with bad privacy practices will be able to generate. In an online context, this means loss of revenue. Consequently, the online industry will be forced to introduce better privacy practices – applied globally. This technology can therefore help to narrow the scope of divergences in the execution of the basic international privacy principles.

Another software product with the potential to bring about international harmonization is called *freedom1.0* recently released by *ZeroKnowledge*.<sup>306</sup> The product makes use of pseudonymous identities for consumers to use when browsing the Net for political, personal (including medical), and business information. A pseudonym is created

---

<sup>302</sup> See Article 29 Working Party, *Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, (Jun. 16, 1998)

<<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11en.htm>>.

<sup>303</sup> Even the World Wide Web consortium views P3P as a complementary tool to laws and self-regulatory programs that can provide enforcement mechanisms rather than an autonomous privacy tool.

<sup>304</sup> Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a technical mechanism for making sure that sites act according to their policies. In addition, P3P does not include mechanisms for transferring data or for securing personal data in transit or storage.

for each separate activity a consumer engages in. This makes it quite difficult for Internet marketers to match profile data to a specific individual.

Intelligent agent tools like that can certainly help to keep Internet interactions anonymous, which would minimize data protection issues.<sup>307</sup> At some point such “anonymizing” software, P3P and OPS might even assure “adequate” protection with respect to data flows from Europe to the United States. Such features may, however, turn out to be elusive where tools like web bugs or cookies try to undercut anonymity - re-establishing the information asymmetry in favor of the industry.

## **5. International Harmonization Through New International Information Privacy Instruments?**

One response to perceived inadequacies of the traditional (OECD and COE) privacy benchmarks has been to call for new international instruments. Proposals to this effect have been brought forward by Greenleaf<sup>308</sup>, Bennett<sup>309</sup>, the International Standards Organization<sup>310</sup>, and Reidenberg.<sup>311</sup>

Reidenberg reasons that despite uniform technical codes he sees fundamental differences persisting in areas where governance norms force a clash of public order. For example, when privacy violations have criminal sanctions for the processing of sensitive

---

<sup>305</sup> The company typically knows far more than the customer about how the information will be used by the company. See, e.g., P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection for Personal Information*, (1997) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

<sup>306</sup> See <<http://www.freedom.net/>>.

<sup>307</sup> See J. Reidenberg, *supra* note 1.

<sup>308</sup> Graham Greenleaf, *Towards an Asia-Pacific Information Privacy Convention*, PRIVACY LAW AND POLICY REPORTER VOL. 2 NO. 7 (1997); and *Global Protection of Privacy in Cyberspace - Implications for the Asia-Pacific*, (paper to the 1998 Internet Law Conference) <<http://www2.austlii.edu.au/itlaw/articles/TaiwanSTLC.html>>.

<sup>309</sup> Colin J. Bennett, Arguments for the Standardization of Privacy Protection Policy: Canadian Initiatives and American and International Responses. *Government Information Quarterly* 14(4): 351-362.

<sup>310</sup> ISO-TMB Ad Hoc Advisory Group on Privacy: An International Standard for Privacy and the Protection of Personal Data, Background Paper, 1998.

data such as medical information, divergences may be hard to co-regulate. Therefore he envisions harmonization through what he calls a “General Agreement on Information Privacy”(GAIP).<sup>312</sup>

His idea to launch such a new type of an international treaty on data protection within the WTO is definitely noteworthy. The WTO certainly offers the institutional process within a wide membership that the Council of Europe failed to provide.<sup>313</sup> However, the major drawback particularly from a European perspective is obvious: Reidenberg’s WTO strategy places data protection in the trade area rather than a political arena. The author acknowledges this and counters that the WTO is increasingly incorporating non-economic values in trade policy. He mentions, for example, that environmental and labor/workers rights issues were topics of discussion at the Seattle Ministerial Conference.<sup>314</sup> This, however, does not necessarily put privacy advocates at ease. Quite understandably many of them still fear that the WTO’s inherent bias toward liberal market norms will shift the issue too far towards a primarily free trade oriented discussion.<sup>315</sup> Reidenberg is confident however, that the breadth of membership in WTO and the growing recognition at WTO that social values are intrinsically linked to trade will cause a blending of governance ideology.<sup>316</sup> He elaborates: “Non-economic values will bring non-market based governance to WTO.”<sup>317</sup> However, an awareness that social values are intrinsically linked to trade does not necessarily mean that the - in privacy

---

<sup>311</sup> See J. Reidenberg, *supra* note 1.

<sup>312</sup> See *id.*

<sup>313</sup> The Council of Europe a Convention has twenty signatory countries. The U.S. is not a signatory of the Convention.

<sup>314</sup> See J. Reidenberg, *supra* note 1, at FN 264.

<sup>315</sup> Tara Lemmey, President of the Electronic Frontier Foundation, presentation at Stanford Law School, Nov. 18, 1999.

<sup>316</sup> See J. Reidenberg, *supra* note 1, at FN 264.

<sup>317</sup> See J. Reidenberg, *supra* note 1.

regulation typical balancing decisions - are made in favor of the socially protection-worthy.

On a more general level, it is worth asking whether it makes sense to go through the trouble of creating a new international agreement. In light of the problems of interpretation, and of application in practice, that arise with the OECD based principles the question becomes why these problems should not arise with any new formulation. Reaching agreement on implementing the already agreed principles is proving difficult enough, without opening up the possibility of disagreement on a revision of the principles.<sup>318</sup>

The difficulties that even countries with similar governance philosophies are facing attempting to align their laws with the EU Data Protection Directive, illustrate that harmonization through international obligations is anything but an easy task. For example, before the EU Commission started drafting the Directive most EU legislators already had statutes specifically dealing with the processing of personal data on the books.<sup>319</sup> In the course of the discussions about new harmonizing legislation, the Commission had to find out that the primary interest of the Member States was not to achieve new, union-wide principles, but rather to preserve their own, familiar rules - very much a pattern underlying the EU – U.S. debate. In fact, the Commission's intervention did not lead to a thorough revision of the traditional concepts. A look at both the original version and the 1992 draft of the Directive reveals that the driving force behind the

---

<sup>318</sup> Nigel Waters, *supra* note 260.

<sup>319</sup> The EU Commission's main concern since the 1970s was to support the development of information and communication technologies in Europe. Therefore any attempt to regulate the use of personal data was initially perceived as potential threat to the promotion of computer based processing. In the Commission's had the view that data, whether personal or not were perfectly normal goods and thus had to be treated in exactly the same way as all other products and services. *See S. Simitis, supra* note 7, at 446.

creation of the Directive was, indeed, the need to combine national laws rather than innovation. For instance, the statement that processing of personal data is lawful only if carried out in accordance with the specific conditions established by the Directive (Article 5), while typical of all German data protection laws, was foreign to a British or Irish reader.<sup>320</sup>

Resulting from these divergences of Member States laws the implementation of the Directive has turned out to be a very slow process. Existing national laws have diverged widely, and even those national data protection authorities with the greatest responsibility and authority, as the French CNIL for example, have lacked the focus and resources necessary to carry out the data protection mandate of their national laws.<sup>321</sup> Not surprisingly therefore, the EU Commission found itself urged to take France, Luxembourg, the Netherlands, Germany and Ireland to the European court of Justice<sup>322</sup> for failure to implement the Directive.<sup>323</sup>

---

<sup>320</sup> On the other hand, the clauses encouraging processors and their associations to establish codes of conduct and the Commission's readiness to accept them as an auxiliary means of regulation (Article 27), while unusual in Germany or France, reflect an approach typical of British and Dutch laws. The provision imposing a duty on a processor to notify the supervisory authority whenever its processing operations are to be wholly or partly automated (Article 18) is a cornerstone of the French data protection law. Finally, the prohibition against processing a series of sensitive data (Article 8), affirms a standpoint shared, for example, by the Belgian, French, Spanish, and Portuguese laws. The prohibition is inconsistent, however, with legislation embodying the German view that "sensitivity" depends on the particular processing context rather than on an abstract classification of the data. *See* S. Simitis, *supra* note 7, at 449, 450.

<sup>321</sup> *See* F. CATE, *supra* note 52, at 47.

<sup>322</sup> *See* EU Commission, *Data Protection: The Commission Takes Five Member States to Court*, (Jan. 11, 2000) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/news/2k-10.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/news/2k-10.htm)>. This step represents the third formal stage of formal infringement proceedings under Article 226 of the EC Treaty. In accordance to the case law of the European Court of Justice (Marleasing case, C-106/89, 13.11.90) individuals are entitled to invoke the Directive's provisions before national courts in those Member States where the implementation legislation is not yet in place. In addition, individuals suffering damage as a result of a Member State's failure to implement the Directive are in some cases entitled to seek compensation before national courts, under the terms of the Court of Justice's case law in the Francovich case (C-6/90 and C-9/90, 19.11.91).

<sup>323</sup> Find Status of Implementation of Directive 95/46 at <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/law/impl.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm)>.

Overall the EU experience shows that harmonization requires a strong coordination of governments to fully align privacy regimes.

#### **D. CONCLUSION**

While some say that electronic media have irreversibly raised the acceptable level of privacy intrusion rendering public expectations of privacy unrealistic<sup>324</sup>, it is still crucial to think about the future of privacy protection in a global context.

The proposition that individuals be empowered to manage their own privacy is seductive in an online context. Disregarding of which governance philosophy, policy-makers should not stand in the way of any such developments. But to rely on this as the only means of privacy protection in the future would be likely to undermine any current level of protection. Individuals are too busy consuming, or working, or just living regular lives to be good at protecting their own interests. It is therefore quite unrealistic to expect individuals to negotiate each and every transaction, to overcome the inevitable power imbalances and to resist the economic incentives that would be offered.<sup>325</sup>

The Safe Harbor Agreement shows that self-regulatory initiatives will play an important role in the future. Given the drawbacks of a purely legislative approach this and different forms of co-regulation could have a potential to enhance privacy protection while harmonizing different privacy implementation regimes. In that context, alternative solutions as reflected in the data protection legislation of New Zealand, Hong Kong and Australia should be considered since they can help to build consensus by drawing upon compatibility points of the diverging regimes.

---

<sup>324</sup> See Dennis Pearce, *Is Privacy Dying?* Australian Press Council News Volume 10 No 4, November 1998.

<sup>325</sup> N. Waters (citing Esther Dyson), *supra* note 318, at 9.

Finding international consensus will be imperative for meeting the challenges of technological and organizational changes. Intergovernmental institutions will and should play a key role in future international discussions. Any discussion of creating new international instruments should also reflect the needs of changed information practices. The debate about intrusive online practices has shown that there is definitely a need to introduce additional international baseline principles - such as those on anonymity.<sup>326</sup> However, the danger of persisting different interpretation of a new set of principles problems remains as long as new instruments do not account for the problems caused by diverging governance philosophies. Privacy advocates will have to play a key role in getting these new factors on the policy agendas of national and intergovernmental decision-takers and focusing attention to underlying governance philosophies.

Overall, international co-operation on how to protect privacy is the right path, but only an effort to address the difference in governance philosophies will provide a functional solution.

---

<sup>326</sup> The online challenge specifically urges to consider the following factors when designing international baseline rules for new national regulations: The privacy implications of new network services should be made fully known to the public; rights for individuals whose personal information is collected should be clearly set out and enforcement of the principles will require legal rights. *See* R. Reilly, *supra* note 186, at 40.

## BIBLIOGRAPHY

### BOOKS

ALLEN ANITA L. & TURKINGTON RICHARD C., PRIVACY LAW, CASES AND MATERIALS (1999).

ASPEN INSTITUTE, TOWARD AN INFORMATION BILL OF RIGHTS, (Firestone Charles M. & Schement Jorge Reina eds.) (1995).

BENNETT J. COLIN, REGULATING PRIVACY DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992).

BRIN DAVID, THE TRANSPARENT SOCIETY (1998).

CATE FRED H., PRIVACY IN THE INFORMTION AGE (Brookings, 1997).

CULLEN INTERNATIONAL, A BUSINESS GUIDE TO CHANGES IN EUROPEAN DATA PROTECTION LEGISLATION (1999).

DIFFIE WHITFIELD & LANDAU SUSAN, PRIVACY ON THE LINE (1998).

DRUCKER PETER FERDINAND, THE CONCEPT OF THE CORPORATION (1946).

EGGER EDELTRAUD, DATENSCHUTZ ALS BÜRGERRECHT IN: DATENSICHERHEIT UND DATENSCHUTZ, (Peter Fleissner & Marcel Choc eds.) (1996).

ETZIONI AMITAI, THE LIMITS OF PRIVACY (1999).

FLAHERTY DAVID H., PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989).

GANDY OSCAR H. JR., THE PANOPTIC SORT (1993).

LANDAU SUSAN & DIFFIE WHITFIELD, PRIVACY ON THE LINE (1998).

LESSIG LARRY, CODE AND OTHER LAWS OF CYBERSPACE (1999).

LINOWES DAVID F., PRIVACY IN AMERICA (1989).

LOEWENHEIM ULRICH/KOCH FRANK A., PRAXIS DES ONLINE-RECHTS (1998).

MACAULAY STEWART, PRIVATE GOVERNMENT, IN LAW AND THE SOCIAL SCIENCES, (Leon Lipson & Stanton Wheeler eds., 1986).

MICHAEL JAMES, PRIVACY AND HUMAN RIGHTS (UNESCO 1994).

PERRI 6 (Demos), THE FUTURE OF PRIVACY, 1 PRIVATE LIFE AND PUBLIC POLICY (1998).

PINCKAERS JULIUS C.S., FROM PRIVACY TOWARD A NEW INTELLECTUAL PROPERTY RIGHT IN PERSONA (1996).

PRIVACY JOURNAL & ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1997).

REGAN PRISCILLA M., LEGISLATING PRIVACY (1995).

REIDENBERG JOEL R. & SCHWARTZ PAUL M., DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996).

SCHWARTZ PAUL M. & REIDENBERG JOEL R., DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996).

SMITH H. JEFF, MANAGING PRIVACY (1994).

SMITH ROBERT ELLIS, PRIVACY, HOW TO PROTECT WHAT'S LEFT OF IT (1979).

SMITH ROBERT ELLIS, THE LAW OF PRIVACY IN A NUTSHELL (PRIVACY JOURNAL, 1993).

SMITH ROBERT ELLIS & PRIVACY JOURNAL, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1997).

SWIRE PETER & LITAN ROBERT E., NONE OF YOUR BUSINESS (Brookings, 1998).

TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Phil E. Agre & Marc Rotenberg eds., 1997).

TURKINGTON RICHARD C. & ALLEN ANITA L., PRIVACY LAW, CASES AND MATERIALS (1999).

WAGNER DECEW JUDITH, IN PURSUIT OF PRIVACY (1997).

WESTIN ALAN, PRIVACY AND FREEDOM (1967).

## **ARTICLES**

### **Legal Periodicals**

Brandeis Louis & Warren Samuel, *The Right to Privacy*, HARV. L. REV. 4, 193 – 220 (1890).

- Bloustein Edward, *Privacy as an Aspect of Human Dignity*, 39 NYU L. REV. 971 (1964).
- Bovenzi Giorgio, *Liabilities of System Operators on the Internet*, 11 BERKELEY TECH.L.J, 1 (Spring 1996) <<http://www.law.berkeley.edu/journals/btlt/>>.
- Bennett Colin J., *Arguments for the Standardization of Privacy Protection Policy: Canadian Initiatives and American and International Responses*, Government Information Quarterly 14(4): 351-362.
- Bennett Colin J., *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 102-05 (Phil E. Agre & Marc Rotenberg eds., 1997).
- Campbell Angela J., *Self-Regulation and the Media*, FED. COMM. L.J. 711.
- Carlson Steven C. & Miller Ernest D., *Public Data and Personal Privacy*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 83 (1999).
- Cate Fred H., *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1 (1998).
- Clarke Roger, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, (Sep. 16, 1999), <<http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>>.
- Gavison Ruth, *Privacy and the Limits of Law*, 89 YALE LAW JOURNAL 421 (1980).
- Gellman Robert M., *Can privacy be regulated effectively on a national level? Thoughts on the possible need for international privacy rules*, 41 VILL. L. REV. 129 (1996).
- Greenleaf Graham, *Towards an Asia-Pacific Information Privacy Convention*, PRIVACY LAW AND POLICY REPORTER VOL. 2 No. 7 (1997);
- Greenleaf Graham, *Global Protection of Privacy in Cyberspace - Implications for the Asia-Pacific*, (1998) <<http://www2.austlii.edu.au/itlaw/articles/TaiwanSTLC.html>>.
- INTERNATIONAL STANDARDS ORGANIZATION, ISO-TMB, Ad Hoc Advisory Group on Privacy: An International Standard for Privacy and the Protection of Personal Data, Background Paper (1998).
- Horwitz Morton J., *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423 (1982).
- Jolish Barak D & Sinrod Eric J., *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1, <[http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_1](http://stlr.stanford.edu/STLR/Articles/99_STLR_1)>.

- Lessig Larry, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 898 (1996).
- Miller Ernest D. & Carlson Steven C., *Public Data and Personal Privacy*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 83 (1999).
- Pearce Dennis, *Is Privacy Dying?* (Australian) Press Council News Volume 10 No 4, Nov. 1998.
- Post Robert, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL.L.REV. 957 (1989).
- Reidenberg Joel R., *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L.REV. 497 (1995).
- Reidenberg Joel R., *The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection*, LEX ELECTRONICA III: 2, (Nov. 1997)  
<<http://www.lex-electronica.org>>.
- Schwartz Paul M., *European Data Protection Law and Restrictions on International Data Flows*, IOWA LAW REVIEW, vol. 80 (1998).
- Schwartz Paul M., *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).
- Shaffer Gregory, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (Winter 2000).
- Simitis Spiros, *From the Market to the Polis: The EU Directive on The Protection of Personal Data*, 80 IOWA L. REV., 445 (1995).
- Sinrod Eric J. & Jolish Barak D., *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, STAN. TECH. L. REV. 1,  
<[http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_1](http://stlr.stanford.edu/STLR/Articles/99_STLR_1)> (1999).
- Waters Nigel, *Re-Thinking Information Privacy - A Third Way in Data Protection?*, in Proceedings of XXIst International Conference of Privacy and Personal Data Protection Commissioners (Sept. 1999)  
<<http://www.pco.org.hk/conproceed.html#top>>.

### **Other Periodicals**

- Alvey Jennifer L., *Coming Soon to a Web Site Near You: Europe's Data Privacy Protection Policy*, BNA ELECTRONIC COMMERCE & LAW REPORT, (Nov. 24, 1999) <<http://www.bna.com/e-law/articles/topstory.html> 11/24/99>.

- Andrews Edmund L., *European Law Aims to Protect Privacy of Personal Data*, N.Y. TIMES, Oct. 26, 1988, at A1.
- Castelli James, *How to Handle Personal Information*, AMERICAN DEMOGRAPHICS 1 (1996).
- Clausing Jeri, *Europe and U.S. Reach Data Privacy Pact*, N.Y. TIMES, (Mar. 15, 2000) <<http://www.nyt.com>>.
- De Bony Elizabeth/Sykes Rebecca, *E.U.-U.S. Privacy Deal Rotten, Observers Say*, INFOWORLD, (Mar.14, 2000) <[www.infoworld.com/articles/en/xml/00/03/14/000314enharbor.xml](http://www.infoworld.com/articles/en/xml/00/03/14/000314enharbor.xml)>.
- Gallagher David F., *Amazon Tries to Ease Privacy Worries*, CYBERTIMES, (Aug. 30, 1999) <<http://www.nytimes.com/>>.
- Greenberg Paul A., *U.S. and EU Reach Data Privacy Accord*, E-COMMERCE TIMES, (Mar. 3, 2000) <[www.ecommercetimes.com/news/articles2000/000315-1.shtml](http://www.ecommercetimes.com/news/articles2000/000315-1.shtml)>.
- McCullagh Declan, *Safe Harbor Swimming in Circles*, WIREDNEWS, (Apr. 29, 1999) <<http://www.wired.com/news/news/politics/story/19414.html>>.
- Oakes Chris, *DoubleClick Plan Falls Short*, WIREDNEWS, (Feb. 14, 2000) <<http://www.wired.com/news/business/0,1367,34337,00.html>>.
- O'Connor Kevin, *The High Cost of Net Privacy*, THE WALL. ST. JOURNAL, Mar. 7, 2000, at A26.
- O'Harrow Robert Jr., *Global Savvy Web 'Bug's' Impact on Privacy Draws Scrutiny Internet: Regulators are looking at stealth tool that tracks online users' activities and soon may be used to identify them by name*, LOS ANGELES TIMES, Nov. 15, 1999.
- Pearce Dennis, *Is Privacy Dying?* (Australian) Press Council News Volume 10 No 4, November 1998.
- Rich Richard C., Griffin Robert J., Friedman Sharon M. *The Challenge of Risk Communication in a Democratic Society*, HEALTH, SAFETY & ENVIRONMENT Vol. 10 No. 3, 189 (Summer 1999).
- Rodger Will, *Poll: Users Wary of Net Ad Targeting*, USATODAY, (Nov. 5, 1999) <<http://www.usatoday.com/life/cyber/tech/ctg585.htm>>.
- Sinrod Eric J. & Jolish Barak D., *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, STAN. TECH. L. REV. 1, <[http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_1](http://stlr.stanford.edu/STLR/Articles/99_STLR_1)> (1999).

Sullivan Denise, *The Right to Privacy Versus the Freedom of the Press: Privacy's Struggle for Equality*, 1 SETON HALL CONST. L.J. 417 (1991).

Sykes Rebecca & De Bony Elizabeth, *E.U.-U.S. Privacy Deal Rotten, Observers Say*, INFO WORLD, (Mar. 14, 2000)  
<[www.infoworld.com/articles/en/xml/00/03/14/000314enharbor.xml](http://www.infoworld.com/articles/en/xml/00/03/14/000314enharbor.xml)>.

## **REPORTS/STUDIES/SURVEYS**

BUSINESS WEEK, *Online Insecurity*, (Mar. 16, 1998).

EPIC, *Critical Infrastructure Protection and the Endangerment of Civil Liberties, An Assessment of the President's Commission on Critical Infrastructure Protection* (October 1998).

EPIC, *Privacy & Human Rights, An International Survey of Privacy Laws and Developments* (1999).

EU COMMISSION, *Handbook on Cost Effective Compliance with Directive 95/46/EC - "Mason Study"*, (August 1998)  
<[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/studies/handbook.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/handbook.pdf)>.

Culnan Mary, *Georgetown Internet Privacy Policy Survey*, (May 1999)  
<<http://www.msb.edu/faculty/culnanm/gippshome.html>>.

Gauthronet Serge & Nathan Frédéric, EU COMMISSION, *On-line Services and Data protection and the Protection of Privacy I*, (December 1998)  
<<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/serve.pdf>>.

GIIC, *ASSESSING DATA PRIVACY IN THE 1990'S AND BEYOND* (1995).

Harris Louis & Associates, Inc. and Westin Alan F., *Commerce, Communication and Privacy Online*  
<<http://www.privacyexchange.org/iss/surveys/computersurvey97.html>>.

Harris Louis & Associates, Inc. and Westin Alan F., *E-Commerce & Privacy: What Net Users Want*, (June 1998) <<http://www.pandab.org/pabsurve.htm>>.

LANDESBURG MARTHA K. ET AL., FTC, *PRIVACY ONLINE: A REPORT TO CONGRESS*, (Jun. 1998) <<http://www.ftc.gov/reports/privacy3/toc.htm>>.

NOAM ELI M., *PRIVACY AND SELF-REGULATION: MARKETS FOR ELECTRONIC PRIVACY* (1997) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>>.

Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, (Washington, 1995).

RAAB, BENNETT, GELLMAN AND WATERS, EU COMMISSION, FINAL REPORT: APPLICATION OF A METHODOLOGY DESIGNED TO ASSESS THE ADEQUACY OF THE LEVEL OF PROTECTION OF INDIVIDUALS WITH REGARD TO PROCESSING PERSONAL DATA: TEST OF THE METHOD ON SEVERAL CATEGORIES OF DATA, (SEPTEMBER 1998) <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/studies/adequat.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/adequat.pdf)>.

REIDENBERG JOEL R. & SCHWARTZ PAUL M., EU COMMISSION, ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY II – REGULATORY RESPONSES, (Dec. 1998) <<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.pdf>>.

SWIRE PETER P., MARKETS, SELF-REGULATION, AND GOVERNMENT ENFORCEMENT IN THE PROTECTION FOR PERSONAL INFORMATION, (1997) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

U.S. Government Working Group on Electronic Commerce, First Annual Report 18 (1998).

WESTIN ALAN F., E-COMMERCE AND PRIVACY: WHAT NET USERS WANT, (June 1998) <<http://www.pandab.org/pabsurve.htm>>.

WESTIN ALAN F. & HARRIS LOUIS & ASS., COMMERCE, COMMUNICATION AND PRIVACY ONLINE, (1997) <<http://www.privacyexchange.org/iss/surveys/computersurvey97.html>>.

### **INTERNATIONAL INSTRUMENTS, POLICY PAPERS, HEARINGS**

Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, <[http://europa.eu.int/eur-lex/en/lif/dat/1995/en\\_395L0046.html](http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html)>.

COE, Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur.T.S.No. 108 <[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/inter/con10881.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm)>.

COE, Recommendation No.R(99) of the Comm. of Ministers, Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways, (Feb. 23, 1999) <<http://www.coe.fr/DataProtection/elignes.htm>>.

OECD, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data <<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>>.

UN Guidelines Concerning Computerized Personal Data Files

[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/inter/un.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/un.htm)>.

Clinton William J. & Gore Albert Jr., A Framework For Global Electronic Commerce,

<http://www.iitf.nist.gov/elecomm/ecom.htm#no.1>>.

Mark Rotenberg, Director EPIC, Testimony and Statement before the Subcommittee on Courts and Intellectual Property, U.S. House of Representatives, Oversight Hearing on Electronic Communications Privacy Policy Disclosures, 570 PLI/Pat 1093.

Deirdre Mulligan, Staff Counsel CDT, Testimony and Statement Before the Subcommittee on Courts and Intellectual Property, Judiciary Committee, U.S. House of Representatives (March 1998).

#### **DOCUMENTS ADOPTED BY THE ARTICLE 29 WORKING PARTY)**

Working Party Recommendation 2/97, *Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet")* (Dec.1997).

Working Party Recommendation 3/97, *Anonymity on the Internet* (Dec. 1997).

Working Party, *Working Document: Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?* (Jan. 1998).

Working Party, *Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries* (Apr. 1998).

Working Party, *Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)* (Jun 1998).

Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (Jul 1998).

Working Party, *Second Annual Report* (Nov. 1998).

Working Party, *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government* (Jan. 1999).

Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (Jul. 1998).

Working Party, *Working Document: Processing of Personal Data on the Internet* (Feb. 1999).

Working Party, *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware* (Feb. 1999).

Working Party, *Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles"* (Jul. 1999).

Working Party, *Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes* (Sep. 1999).

### CASES

Clyatt v. United States, 197 U.S. 207, 216-20 (1905).

Evans v. Newton, 382 U.S. 296, 299 (1966).

Marsh v. Alabama, 326 U.S. 501, 507-08 (1946).

Mc Veigh v. Cohen, 983 F. Supp. 215 (D. D.C. 1998).

NAACP v. Alabama, 357 U.S. 449 (1958).

New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964).

Travis v. Reno, 163 F 3d 1000, 1002 (7th Cir. 1998).