2000

Raising or Razing the E-Curtain: The EU Directive on the Protection of Personal Data

Kevin Bloss

Notes

Raising or Razing the e-Curtain?: The EU Directive on the Protection of Personal Data

Kevin Bloss

On October 25, 1998, the EU passed Directive 95/46/EC ("Directive") establishing comprehensive standards for the protection of personal data throughout the 15-member European community.[1] The main goal of the Directive is to provide a framework for EU countries to adopt comparable domestic laws that will prevent the unauthorized dissemination of its citizens' personal information amongst various companies both inside and outside the EU.[2]

Data privacy for personal information in the EU has been a growing concern since the early 1970's.[3] Several of the member nations have adopted domestic, privacy-protection statutes imposing wide-ranging affirmative obligations on both the country's public and private sectors.[4] The Directive is seen as an effort to help harmonize domestic laws in order to promote a unified market within the EU and avoid disputes which could ultimately lead to state-imposed data blockages between member nations.[5]

The Directive will also greatly affect countries outside the European Union. With the advent of the Internet, the ease of conducting business and the ease of gathering information on a world-wide level has pushed the requirements of this Directive

1. *See* W. Scott Blackmer et al., *Online Consumer Data Privacy Regulation in the U.S.*, ELEC. BANKING L. & COM. REP. Apr. 1999, at 1.

2. *See* Henry J. Perritt, Jr. & Margaret G. Stewart, *False Alarm?*, 51 FED. COMM. J.L. 811 (1999).

3. *See* Peter P. Swire, *Of Elephants, Mice and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 1001 (1998); *see also* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32 (1997). The German State of Hesse enacted the first data protection statute in what is now the Europe Union in 1970. *See id.*

4. *See* Swire, *supra* note 3.

5. *See id.*

to the international forefront.[6] Therefore, while the Directive is an attempt to create uniformity within the European Union, its strict provisions for the protection of personal data will also be required of all foreign entities that wish to do business within the Union.[7] This unilaterally-decided, extraterritorial effect has been the impetus for the burgeoning debate between the European Union and the rest of the world.[8] Today, many sectors of the U.S. market, as well as other markets world-wide, are not in compliance with the Directive.[9] Although ample opportunity for negotiation among all the concerned parties exists, if no compromise is struck, many areas of the world market could conceivably be denied access to European customers. The resulting interruption in data flow, while obviously hurtful to businesses in non-compliant areas of the world, will also adversely affect European countries by decreasing their total amount of commerce.[10] The market pressures and their potential effects on countries exemplify that the debates over the Data Privacy Directive must reach some sort of accord, be it through a compromise or a dispute resolution. Without a resolution the stand-off could result in an extreme hindrance to global trade leaving all major trading countries in an unfavorable economic state.[11] This, consequently, could cripple the further development of electronic-commerce technology.

This Note will show the potential likelihood that ruminations over this Directive will ultimately put it under the scrutiny of a WTO dispute settlement panel. Part I of the Note will lay out the basic structure of the Directive, highlighting the articles which have and will likely continue to spawn the most debate between the EU and the United States. Part II will show that the EU and U.S. are not so diametrically opposed in their approaches to privacy regulation, as one would first assume. However, this note will also highlight some key problems behind resolving this potentially devastating conflict which makes it

6. *See* Swire, *supra* note 3, at 1008. It is very possible that the problem the Internet creates in relation to this directive was not even considered when the Directive was formed because its drafting occurred in the early nineties. *See id.*

7. *See*, Gary E. Clayton, *Manager's Journal: Eurocrats try to Stop Data at the Border*, WALL ST. J., Nov. 2, 1998, at A34.

8. *See* Perritt & Stewart, *supra* note 2, at 812.

9. *See* Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L.J. 2024, 2034 (1999).

10. *See* Perritt & Stewart, *supra* note 2, at 820.

11. *See id.*

difficult to see any possibility of an accord between the EU and the U.S. Part III of this Note will attempt to read the tea-leaves by discussing both how this conflict could find itself in front of the WTO, and some of the issues a WTO panel would consider if asked to hear this case.

I. Basic Structure of the Directive

The Data Privacy Directive was an early 1990 response to a growing number of domestic privacy laws that arose in Europe throughout the 1970's and 1980's.[12] The Directive, being merely procedural, has little control in directing EU member-nations to adopt domestic laws that conform to the Directive's provisions.[13] This important distinction shows that, even though the Directive is in force, many of the required domestic laws have yet to be created, thus leaving room for potential negotiations among interested parties.

The Directive's privacy requirements pertain to all processing of personal data. "Processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means."[14] "Personal data" is also defined broadly as "any information relating to an identified or identifiable natural person ('data subject')."[15] Any time data is processed, collectors must notify the data subject of their identities, and of the intended use for the information being gathered.[16] The data can then only be used with regard to the purposes for which it was obtained.[17] Moreover, data subjects have the right to opt out before a collector can give their information to third parties for other marketing purposes.[18] Data subjects also have the right to access their personal data and correct any errors that may be found.[19] These requirements apply to all data collectors regardless of EU status.

---

12. *See* Pearce & Platten, *supra* note 9, at 2024-2026.

13. *See* Swire, *supra* note 3, at 994 (explaining that the resultant legislation adopted by the various member-states must comply with the Directive and will take precedence over any preexisting domestic laws with which it is in conflict).

14. Council Directive 95/46/EC, 1995 O. J. (L281) 31 (visited Feb. 20, 2000) <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>.

15. *Id.*

16. *See id.*

17. *See id.*

18. *See id.*

19. *See id.*

Perhaps the most controversial part of the Directive is Article 4, which deals with choice of law provisions for the member states.[20] The directive allows EU countries to apply their national provisions against any entity violating privacy rules within that country, regardless of the entity's nationality.[21] In particular, Article 4(1)(c) of the Directive brings under its purview any data collector who "makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."[22] While much of the Directive presents problems for non-EU companies wishing to do business or locate part of their operations in the EU, this provision implies that any individual gaining access to EU consumers via as little as a computer screen within the Union will be held liable if they transfer any personal information out of the EU.[23] The ongoing debate as to the exact meaning of Article 4(1)(c) and the practical difficulties in enforcing it on every non-compliant party that gains access to EU consumers on the Internet continues to gain momentum.[24]

Articles 25 and 26 of the Directive deal with transfers to third-party countries.[25] Article 25 allows transfers to third-party countries upon approval that those countries have adequate levels of data protection.[26] Article 26 covers a series of exceptions ("Derogations") to Article 25 allowing for data transfer between the EU and third-party countries despite their lack of adequate data protection.[27] These exceptions range from unambiguous consent of the data subject to individual contractual agreements on privacy. However, each member state has the right to nullify these exemptions if they so choose when passing this or other domestic laws.[28]

---

20. *See* Council Directive 95/46/EC, 1995 O. J. (L281) 31 (visited Feb. 20, 2000) <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>.

21. *See id.*

22. *Id.*

23. *See* Swire, *supra* note 3, at 1007. It is also important to remember the breadth with which "personal data" is defined in Art. 2 of the Directive to fully appreciate the scope of Art. 4. *See supra* note 14.

24. *See id.*

25. *See* Council Directive 95/46/EC, 1995 O. J. (L281) 31 (visited Feb. 20, 2000) <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>.

26. *See id.*

27. *See id.*

28. *See id.* "By way of derogation from Article 25 *and save where otherwise provided by domestic law governing particular cases*, Member States shall

To enforce these and other provisions, each member nation must create at least one supervisory authority able to intervene for individuals and bring violations to the attention of the proper judicial authorities.[29] The Directive allows these authorities to block, erase or destroy data, impose bans on processing, warn or admonish the controller, or refer the matter to the national parliaments or other political institutions.[30] In the end, non-compliance could lead to destruction of important data, blockage of access to the EU market, and ultimately legal proceedings against entities which fail to meet Directive requirements; all of which causing significant economic harm.[31]

Whether an entity meets the requirements mentioned above is to be determined by the laws of the EU country where it does business.[32] To aid countries in their decision-making process, the Directive has created two advisory bodies: 1) one that can provide advice on all matters of the Directive ("The Working Party");[33] and 2) another that can choose to implement this advice through a weighted vote of its members ("The Committee").[34] For example, if an EU member-nation has ruled, with the advice of The Working Party, that the United States or a sector of the United States has inadequate privacy measures, that decision could then be appealed to the Committee established under Article 31 for a judgment on adequacy.[35] The Committee then votes and releases a binding ruling.[36]

---

provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25. . . ." *Id.* (emphasis added).

29. *See id.*

30. *See id.*

31. *See* Council Directive 95/46/EC, 1995 O. J. (L281) 31 (visited Feb. 20, 2000) <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>. *But see* Swire, *supra* note 3, at 999. "Supervisory authorities have usually worked informally with controllers when complaints are filed. In many instances, the controller explains why the practice in fact complies with applicable standards or else agrees to modify the objectionable practice. This non-litigation approach is likely to predominate under the Directive as well." *Id.*

32. *See* Council Directive 95/46/EC, 1995 O. J. (L281) 31 (visited Feb. 20, 2000) <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>.

33. *See id.*

34. *See id.* at art. 31. The voting procedure is set up so that the larger EU member-nations have a greater vote. *See id.* The decisions of this body are then binding on all interested parties. *See id.*

35. *See* Swire, *supra* note 3, at 1005.

36. *See id.*

At first blush, it appears that these advisory bodies can usurp the authority of EU member nations; however, the purpose of their creation was to help encourage a harmonization of privacy laws among the member states.[37] Theoretically, if all member-nations adopt the appropriate privacy laws pursuant to the Directive, the rulings of the advisory bodies created within the Directive should never conflict with the domestic law of the member-states. With this in mind, it appears that the creators of the Directive intended these bodies to be merely supplemental in nature and not in any way controlling over the member nations to the extent of superceding domestic laws.

II-A. Problems that may arise under the EU Directive

One of the strongest and most persistent objectors to the EU Directive is the United States. The United States and its companies refuse to acknowledge personal data privacy as a fundamental human right.[38] However, it is important to note the U.S. is not completely insensitive to data privacy. In fact, there are several federal statutes in various sectors of consumer and corporate practices which address data privacy.[39] Unfortunately, these statutes are far from comprehensive and do not allow the United States to claim that it meets the Directive's data privacy requirements as a nation.[40]

The differing points of view about privacy rights between the U.S. and the EU have led to key differences in the two entities' approaches to privacy that will make reconciliation of conflicts regarding the Directive difficult. First of all, the U.S. approach to privacy, while recognizing its growing importance in the eyes of the U.S. consumer,[41] also realizes certain undeniable

37. *See id.* at 1004.

38. *See* Pearce and Platten, *supra* note 9, at 2047. "There appears to be a reluctance on the part of the U.S. companies to acknowledge that privacy is a fundamental human right that needs to reconciled with legitimate business interests." *Id.*

39. *See* Blackmer et al., *supra* note 1, at 1. These statutes include FCRA (Fair Credit Reporting Act, 15 U.S.C. § 1681), COPPA (Children's Online Privacy Protection Act 1998, §§ 1302(1), 1303(b)(1)), and others which protect the privacy of certain types of information such as the Electronic Communications Privacy Act (18 U.S.C. § 2510), and the Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227). *See id.* at 6-7.

40. *See* Perritt & Stewart, *supra* note 2, at 812.

41. *See* Pearce & Platten, *supra* note 9, at 2025. "In the United States, several recent consumer surveys have highlighted both a high degree of pubic concern about privacy and skepticism about the effectiveness of existing U.S. data protection practices." *Id.* (citing Louis Harris & Alan Weinstein, *Com-*

economic advantages to be gained from collection and use of personal information.[42] With this relationship in mind, the U.S. has developed a laissez-faire approach to most privacy regulations, allowing the various sectors to work privately with consumers to create an adequate system of protection.[43] Unlike the EU system, which focuses on the rights of consumers over the importance of economic streamlining, the U.S. system attempts to ensure that both interests are legitimately represented as regulations are created.[44]

As a consequence of this laissez-faire approach, and the rise in consumer concern over privacy, a spate of self-regulatory bodies have arisen around the U.S., primarily in relation to corporate Internet activities.[45] These bodies, such as TRUSTe,[46] BBBOnline[47] and other industry-led groups set up privacy regulations for member corporations and then monitor those corporations to ensure that the regulations are being followed.[48] By creating standards which all of the members agree to obey, these self-regulating bodies also expose their members to possible enforcement by the Federal Trade Commission (FTC) for failure to meet their self-prescribed rules.[49] The FTC, while having little power to enforce independent privacy rules, reserves the power to enforce any company's self-prescribed privacy regulations if it feels that the company is deviating from their privacy promises.[50]

---

merce Communications and Privacy Online: A National Survey of U.S. Computer use, Privacy laws and American Business (1997)).

42. *See* Jonathon P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U.L. REV. 1183, 1187 (1999). The creation of "[t]ailored advertising [(via collection of personal data)] can be vital to the growth of electronic commerce because, as marketing costs fall, more companies will begin to conduct more commerce over the Internet, which in turn will lead to lower overall prices for consumers around the world." *Id.*

43. *See id.* at 1203.

44. *See id.*

45. *See* Blackmer et al., *supra* note 1, at 1.

46. *See* Cody, *supra* note 42, at 1220. "TRUSTe is a non-profit initiative sponsored by companies such as Microsoft, IBM, AT&T, Excite and Compaq, that provides oversight functions to ensure that its members are following their posted privacy policies." *Id.* at 1220-21.

47. *See id.* at 1222. BBBOnline is a similar entity to TRUSTe initiated by the Better Business Bureau that awards seals of approval to companies that meet specified privacy requirements. *See id.*

48. *See* Blackmer et al., *supra* note 1, at 1.

49. *See id.* at 5.

50. *See id.* at 3-4. Pursuant to the Federal Trade Commission Act, 47 U.S.C. § 45, the FTC has the right to investigate and enjoin any unfair or deceptive conduct in nearly any industry which affects interstate commerce. The

One example of this enforcement is the *Geocities* case.[51] In this case, the FTC accused the Geocities website of engaging in illicit practices with its collection and use of personal information from its online customers.[52] Geocities denied the allegations, but ultimately conformed its operations to the FTC standards being demanded in the proceedings.[53]

These self-regulatory bodies are not without problems, however. If the FTC fails to act, individuals are left with no legal recourse against the violating companies.[54] If the FTC does act, however, there can still be problematic results in terms of creating privacy regulations. While certain companies will look to the *Geocities* case as a benchmark for setting up privacy systems,[55] others will see this as an excellent reason to avoid privacy policies all together.[56] Also, it is important to note that the self-regulating bodies could be reluctant to report any of the member companies to the FTC (especially the prominent ones) at the risk of losing their corporate sponsorship.[57]

Another problem that highlights the inability of the U.S. and the EU to see eye-to-eye on the Directive is the hierarchy of their legal systems. In the U.S., the courts are, for the most part, the supreme arbiters and interpreters or the law. Americans often look to the courts for answers to the scope and application of statutes and common laws. When powers are delegated to administrative bodies, there must be an absolute delegation of power before a court will observe the administrative advice. Even then, courts can approach administrative advice with skepticism. In the EU there is a much greater trust and dependence on administrative bodies; their decisions tend to carry more weight and they have better working relations with European courts of law.[58]

---

right to investigate a company's self-prescribed data privacy standards is commensurate with the acts this statute grants. *See id.*

51. *See id.*; *see also* Federal Trade Commission, *In the Matter of GeoCities: Complaint* (visited Oct. 17, 1999) <http://www.ftc.gov/os/1998/9808/geo – cmpl.htm>.

52. *See* Cody, *supra* note 42, at 1226.

53. *See* Blackmer et al., *supra* note 1, at 4 - 5.

54. *See* Cody, *supra* note 42, at 1225.

55. *See* Blackmer et al., *supra* note 1, at 5.

56. *See* Cody, *supra* note 42, at 1226. Avoiding self-prescribed privacy rules also avoids any FTC involvement with your company on privacy grounds. *See supra* note 42, and accompanying text.

57. *See id.* at 1227.

58. *See* Pearce & Platten, *supra* note 9, at 2025.

Both the recognition of the importance of markets and the comparative distaste for giving administrative bodies too much power, make it difficult to predict any easy solution to the dilemma that the Directive presents. From a practical standpoint both entities will try to persuade the other towards compromise. From a strategic standpoint, the EU could accept some of the U.S. sector-based privacy regulations as "safe-harbors," thus giving certain companies within an industry a competitive advantage over other companies without adequate data privacy protection.[59] Theoretically, this will create an incentive for the non-compliant companies to create proper regulations.[60] However, many U.S. companies may attempt to circumvent the Directive by creating individual contracts with various parts of the EU market agreeing to the required data protections.[61] There also remains the chance that the EU plans back-fire and various parts of the world purposely avoid complying with the standards in an effort to make a political statement about the privacy requirements.[62]

II B. Possibilities for Resolution

Even though the EU and U.S. seem light years apart in resolving this issue, there is room for compromise. The national regulations and regulatory bodies that will be formed by the EU pursuant to this Directive are still in developmental stages.[63] It is quite possible that EU countries could work with foreign corporations within its borders when developing their domestic laws.[64] The EU has shown before that it is willing to move on these issues.[65] This is evidenced by the constant reductions in rigidity of the Directive throughout its development over the last decade.[66] The EU must also take into account the fact that the U.S. is the leading power in the Internet industry. To coldly re-

59. *See id.* at 2049.
60. *See id.* at 2049.
61. *See id.* at 2048.
62. *See* Pearce & Platten, *supra* note 9, at 2034.
63. *See supra* Part I.
64. *See* Swire, *supra* note 3, at 1020. "[A]nalysis suggests that national data protection rules might work reasonably effectively where the data is primarily in the hands of the largest companies." *Id.*
65. *See* Matthew J. Feeley, *The Rise of Self-Regulation*, 22 B.C. INT'L & COMP. L. REV. 159, 171 (1999). This article posits that the EU made a shift closer to the idea of self-regulation shortly after a speech by President Clinton which advocated self-regulation as the proper approach to data privacy issues. *See id.*
66. *See id.*

ject any offers at long-term compromises could lead to an inability of EU companies to take advantage of Internet-related economic opportunities in the U.S. .[67]

The U.S. also has room to improve by increasing the responsibility of the FTC. As stated, the FTC already engages in a form of overview on privacy protection regulations, so it is possible that these responsibilities can be increased in the hopes of a compromise. One method that immediately presents itself is to set up a system whereby corporations by default, adopt a set of FTC-ordained obligations on privacy protection. The corporations would not be forced to adopt the measures, they would simply have to clarify their intentions to adopt alternative measures and not participate in the FTC system. It is likely that inertia and public perceptions would play a large role in this system. Companies may be reluctant to publicly reject the basic privacy principles of the FTC, or simply may be unwilling to go to the trouble of creating their own guidelines.

Another idea would be to include discussions on this issue in the next GATT/WTO negotiation rounds.[68] However, this presents problems because the trade negotiators may not be experienced in the methods of privacy law and the issue could prove to be such a sticking point that it might significantly hinder the negotiations altogether.

III. The Directive and the WTO

On a larger scale, the U.S. could also attack the Directive as a barrier to trade and a violation of the WTO Agreement.[69] Advisers to President Clinton have stated that if the EU and the U.S. cannot work out their differences concerning the Directive, the U.S. will challenge the legitimacy of the Directive's extraterritorial control by going to the WTO.[70] The resultant decision by the WTO is difficult to predict because such a decision relies heavily upon the facts of the particular case through which the U.S. would challenge the Directive.[71] Nonetheless, when looking at various prohibitions under the GATT and some past deci-

67. *See id.* at 171-72.

68. *See* Swire & Litan, *supra* note 3, at 189.

69. *See* Perritt & Stewart, *supra* note 2, at 820-21. These regulations "are tantamount to discrimination against trade in goods or services with foreign countries." *Id.*

70. *See* Swire and Litan, *supra* note 3, at 189. Ira Magaziner adviser to President Clinton stated the intentions of the U.S. to involve the WTO in this dispute at a conference at the Brookings Institute on February 6, 1998. *See id.*

71. *See id.* at 192.

sions made by various GATT/WTO panels, one can extrapolate certain situations where the EU Directive could conflict with the EU's previously-agreed-to GATT obligations.

One area where the EU Directive appears to directly conflict is the Most Favored Nation obligation (hereinafter "MFN") agreed to in the GATT.[72] The MFN clause states that all contracting parties to the GATT/WTO must afford identical privileges to every other contracting party with respect to any given product either imported into or exported out of its country.[73]

For example, imagine a product that requires customer information for its sales and distribution around the world. Assume that this information is gathered on a large-scale basis thereby negating any possibility for personal consent to the company's data collection.[74] One such industry that fits this description and has already suffered national enforcement of the Directive is the U.S. airline industry.[75] The particular airline in this situation was forced by Swedish privacy authorities to create a bifurcated database: one database for EU citizens with adequate privacy protections and one database for the rest of the world.[76] While Sweden's prohibitions may have left the U.S. airline industry with little recourse but to alter their database, the U.S., as a contracting party to the GATT, could challenge the measure as a violation of GATT provisions.[77]

---

72. *See* General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, T.I.A.S. 1700, 55 U.N.T.S. 194 [herinafter GATT].

73. *See id.* The MFN clause states in relevant part,

> with respect to all rules and formalities in connection with importation and exportation, . . . any advantage favour, privilege or immunity granted by any contracting party to any product originating in or destined for any other country shall be accorded immediately and unconditionally to the like product originating in or destined for the territories of all other contracting parties.

Id.

74. *See* Council Directive 95/46/EC, art. 10, 1995 O.J. (L281) 31 (visited Feb. 24, 2000) http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm; *see also supra* Part I.

75. *See Review & Outlook*, Editorial, WALL ST. J., June 21, 1999, at A26. "American Airlines was forced to stop transmitting information — such as meal preferences or requests for wheelchair assistance – about European passengers to the company's Sabre reservation system in the U.S. after Sweden's national privacy watchdog forced the airline to set up a separate database." *Id.*

76. *See id.*

77. *See* GATT art. XXIII(2). Article XXIII(2) states,

> If any contracting party should consider that any benefit accruing to it directly or indirectly under this Agreement is being nullified or impaired or that the attainment of any objective of the Agreement is being impeded as the result of (a) the failure of another contracting party to carry out its obligations under this Agreement, or (b) the application

The strength of the U.S. claim would be greater if the U.S. could establish to the WTO that airlines in other countries were not subject to the same prohibitions as the U.S. airline industry. If the U.S. showed that other WTO members have airlines with open access to the personal information of European citizens, it would have a strong argument that its airline ticket industry is entitled full access to the EU air-passenger market.[78] Using GATT terminology, the U.S. could maintain that the EU Directive is a rule or formality which creates a privilege or immunity for the export of airline tickets from contracting parties that meet the Directive requirements. Such privilege and immunity should be accorded immediately and unconditionally to other contracting parties with regard to airline tickets according to GATT Article I.[79]

The airline industry is just one of many possible examples through which the U.S. could challenge the Directive's validity under the GATT. Any product subject to different treatment by the EU, based on the Directive's prohibitions, will leave the EU with little to argue before a WTO panel. Past MFN decisions have held that the burden of proving discriminatory treatment lies with the parties claiming discrimination.[80] Although many MFN cases only deal with disputes over tariff application to products, the broad scope of the language in the MFN clause seems to imply that methods of decision-making adopted by these WTO panels would easily apply to other factors affecting trade, such as rules or regulations.[81] If the U.S. could establish its complaint by meeting the burden set out by earlier panels, the U.S. would legitimize its challenge of the Directive under the MFN clause.

When rendering MFN clause decisions, WTO panels always consider whether the product subject to the alleged discrimina-

---

by another contracting party of any measure, whether or not it conflicts with the provisions of this Agreement, or (c) the existence of any other situation, . . . the matter may be referred to the CONTRACTING PARTIES [(i.e. WTO panel)]. The CONTRACTING PARTIES shall promptly investigate any matter so referred to them and shall make appropriate recommendations to the contracting parties.

78. *See supra* note 73 and accompanying text.

79. *See id.*

80. 79 *See* Japan – Tariff on Import of Spruce-Pine-Fir (SPF) Dimension Lumber, July 19, 1989, GATT B.I.S.D. 167 (1990). "A contracting party which claims to be prejudiced [(under MFN obligations)]. . . bears the burden of establishing that such tariff arrangement has been diverted from its normal purpose so as to become a means of discrimination." *Id.*

81. *See supra* note 73 and accompanying text for scope of MFN clause's application.

tion is a "like product" to the product benefiting from the regulation or tariff in question.[82] This is often a difficult determination to make. To do so, panels usually consider such things as methods of production and a product's particular uses.[83] Panels dealing with MFN claims have also created an interesting juxtaposition by acknowledging the importance of letting the importing country make its own classifications for product tariffs, and also acknowledging the importance of uniformity among national classifying systems.[84]

When arguing before a WTO panel, the EU could rely upon the mixed signals on how products are properly classified as a defense. The EU could argue that, according to their classification system, products imported into the Union without adequate privacy safeguards are different than products imported with adequate privacy safeguards. However, when one considers that the products being compared will likely be nearly identical and used for the same purpose, the EU's separate classification would likely be discriminatory treatment.

If the panel does not find a GATT violation from an MFN argument, the U.S. could also argue that the Directive has nullified or impaired anticipated benefits under the GATT.[85] In or-

82. *See* Spain – Tariff Treatment of Unroasted Coffee, June 11, 1981, GATT B.I.S.D. (28th Supp.) at 102 (1982). Spain attempted to apply different tariffs to various types of coffee beans based on differences in the imported coffee due to geographical factors and cultivation methods for the various beans. The panel hearing the case rejected these factors as legitimate methods of differentiation and found that since the beans were often used in tandem to make various coffee blends they should not be subject to differing tariffs. *See id.*; see *also* Treatment By Germany of Imports of Sardines, Oct. 31, 1952, GATT B.I.S.D. (1st Supp.) at 53 (1953). Although not ultimately considered by the panel when it reached its decision, like product analysis was argued by both parties to the dispute and the panel acknowledged its importance in MFN analysis. *See id.*

83. *See* Spain – Tariff Treatment of Unroasted Coffee, *supra* note 81. The Spanish Coffee decision considered the different types of coffee beans to be similar under tariff schedules partially because the beans were manufactured together into coffee blends and also because the end use of all the beans was coffee consumption. *See id.*

84. *See* Japan – Tariff on Import of Spruce—Pine—Fir (SPF) Dimension Lumber, *supra* note 79. "[I]f a claim of likeness was raised by a contracting party in relation to the tariff treatment of its goods on importation by some other contracting party, *such a claim should be based on the classification of the latter, i.e. the importing country's tariff.*" *Id.* (emphasis added).

85. *See* Treatment by Germany of Imports of Sardines, *supra* note 81. The panel focused on Norway's loss of anticipated benefits under the GATT when it found Germany to be in violation of the agreement. *See id.*.

der to establish a nullification or impairment[86] of anticipated benefits the U.S. would have to establish that the Directive's enforcement has changed the competitive conditions for the specific product in the EU.[87] They must also show that such a change could not reasonably have been anticipated by the U.S. Government when it entered into trade negotiations.

Theoretically, any impairments that the U.S. could claim were caused by the Directive (either under MFN or under Nullification or Impairment) do not even have to be part of a previously agreed to multilateral tariff reduction schedule.[88] The MFN clause states only that all contracting parties have a right to equal treatment on like products being imported into or exported out of another contracting party's territory.[89] Also, claims of nullification or impairment under the GATT can be made by simply stating that "the attainment of [an] objective of the Agreement is being impeded as the result of . . . the application by another contracting party of any measure whether or not it conflicts with the provisions of this Agreement." In either circumstance, the U.S. could say that the Directive is a serious detriment to the GATT's principle objective of trade liberalization.[90]

---

86. *See* GATT art. XXIII (1). The nullification and impairment clause states in relevant part,

> If any contracting party should consider that any benefit accruing to it directly or indirectly under this Agreement is being nullified or impaired or that the attainment of any objective of the Agreement is being impeded as the result of
>
> (a) the failure of another contracting party to carry out is obligations under this Agreement, or
>
> (b) the application by another contracting party of any measure, whether or not it conflicts with the provisions of this Agreement, or
>
> (c) the existence of any other situation,
>
> the contracting party may, with a view to the satisfactory adjustment of the matter, make written representations or proposals to the other contracting party or parties which it considers to be concerned. Any contracting party thus approached shall give sympathetic consideration to the representations or proposals made of it.

Id.

87. *See* Treatment By Germany of Imports of Sardines, *supra* note 81; *see also* The Australian Subsidy on Ammonium Sulphate, Apr. 3, 1950, GATT/CP/4/39 188 (1950).

88. *See supra* note 73 and accompanying text.

89. *See id.*

90. *See* GATT preamble. The preamble states that in order to, among other things, develop and expand the production and exchange of goods worldwide, the participating governments are "desirous of contributing to these objectives by entering into reciprocal and mutually advantageous arrangements

In addition, the U.S. may have a valid claim under the General Agreement on Trade in Services[91] (GATS).[92] Similar to the GATT, the GATS also contains an MFN clause. An impairment argument under the GATS more closely fits with the nature of the Directive because data collection is itself not a product, but a service. Also, collection of personal data is more often used by businesses providing services, such as a contracting service, that would need to know personal information from future employers to effectively bid on certain jobs.[93] The principle problem with claiming damage under the GATS is that it contains an exception for the enforcement of personal privacy rules.[94] However, this exception is limited, by the requirement that the privacy measures are not applied in an arbitrary or discriminatory method.[95] The EU would likely still rely heavily on this exception if involved in a GATS claim, and the U.S. would carry an additional burden of proving that the exception does not apply to this MFN dispute. That additional burden would not exist if the U.S. could bring a claim under the GATT.

Even if the U.S. receives a favorable decision from the WTO, this will not remove the Directive from the EU legal world. In fact, the EU remains very adamant about maintaining its privacy standards.[96] What the U.S. will gain out of a favorable

---

directed to the substantial reduction of tariffs and other barriers to trade and to the elimination of discriminatory treatment in international commerce." *Id.*

91. *See* Swire & Litan, *supra* note 3, at 190.

92. *See* General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization [herinafter WTO Agreement], Annex 1B. LEGAL INSTRUSMENTS – RESULTS OF THE URUGUAY ROUND vol. 31; 33 I.L.M. 81 (1994) [herinafter GATS].

93. *See* Swire & Litan, *supra* note 3, at 190. Swire and Litan posit that if two different third countries had companies competing for the same contract and the EU chose to prohibit one of the companies based on the Privacy Directive, the country in which the rejected company is located could claim under the MFN principle of the GATS, especially if that country's privacy regulations were not that different than the accepted country. *See id.*

94. *See* GATS art. XIV. This article states in relevant part,

> nothing in this agreement shall be construed to prevent the adoption or enforcement by any Member of measures . . . (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: . . . (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality or individual records and accounts.

Id.

95. *See* Swire & Litan, *supra* note 3, at 191.

96. *See Review & Outlook*, *supra* note 75. John Mogg, representing the EU position on the Directive at a conference for American and Italian business executives, stated, "One of the myths to be dispelled is that you can develop the

finding from the WTO is principally two-fold. First, a favorable finding will allow the U.S. to legitimately begin suspending its concessions to the EU in the amount equivalent to its estimated losses from trade prohibitions caused by the Directive's enforcement.[97] Second, as the U.S. and the EU attempt to negotiate some sort of an accord on the personal privacy issue, the EU will be less reticent to seriously consider the self-regulatory system under which the U.S. runs its personal data privacy regulations.[98]

There is also value in demonstrating to the rest of the world that you are the correct party. The U.S. is the world leader in information technology and has considerable control over determining the privacy protocols to be used in much of the software distributed around the world.[99] With the WTO ruling in its favor the U.S. could more easily encourage the rest of the world to take its side and avoid adopting privacy rules which have already run afoul of the GATT. The EU, in response, could argue, as discussed above, that there exists a growing trend towards data protection in the WTO with the advent of the GATS and urge further improvement to guarantee even more data protection throughout the WTO community.[100]

IV. Conclusion

As e-commerce grows, without harmonization between the U.S. and the EU on the Data Privacy Directive, one of the two economic super-powers of the world could be left isolated in many facets of the global economy.[101] To achieve compromise, both sides will need to recognize the structure of the other's system. The EU must recognize the importance that the U.S. places on letting the market play a role in regulation,[102] and the

---

full potential of the net without rules." *Id.* He further noted, "The Wild West Web is not an option." *Id.*

97. *See* GATT art. XXIII. Article XXIII states,

> [i]f no satisfactory adjustment is effected between the contracting parties concerned within a reasonable time . . . [and] the CONTRACTING PARTIES consider that the circumstances are serious enough to justify such action, they may authorize a contracting party or parties to suspend concessions or other obligations under this Agreement as they determine to be appropriate in the circumstances.

Id.

98. *See* Blackmer et. al. *supra* note 1, at 4 –5.
99. *See* Pearce & Platten, *supra* note 9, at 2050.
100. *See* Pearce & Platten, *supra* note 9, at 2051.
101. *See* Pearce & Platten, *supra* note 9, at 2034.
102. *See* Swire, *supra* note 64, and accompanying text.

U.S. must acknowledge that the creation of an administrative body to oversee the enforcement of privacy regulations may be a necessary evil to monitor a system of such magnitude.