ARTICLES

THE LAW REGULATING UNSOLICITED COMMERCIAL E-MAIL: AN INTERNATIONAL PERSPECTIVE

John Magee[†]

Advertising is a valuable economic factor because it is the cheapest way of selling goods, particularly if the goods are worthless.

—Sinclair Lewis (1885–1951)

Advertisements on the current Internet computer network are not common because of the network's not-for-profit origins.

—Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 1994

I. INTRODUCTION

The sending of unsolicited commercial e-mail, or spam, to Internet users has been a major problem since the early days of the Internet. By shifting the costs involved with the sending of bulk e-mail, unscrupulous advertisers have been able to mass market their products for a nominal cost and in doing so, have attracted the wrath of individual users, Internet service providers and various interested groups, agencies and organizations. A cursory examination of some

† John Magee BCL, LLM [jonnermagee@yahoo.com] is from Dublin, Ireland. He studied Law at University College Dublin before going on to complete a Master's degree in Computers and Law at the Queen's University, Belfast. The author would like to thank Dr. Philip Leith at Queen's University, Prof. Giovanni Sartor at the University of Bologna, and Aoife Brophy of Trinity College Dublin for all of their generous assistance during the writing of this Article.

of the statistics associated with unsolicited commercial e-mail is a helpful starting point in identifying some of the problems associated with this phenomenon and its regulation. A 1998 Novell report estimated that the annual cost of spam to British and Irish business, in terms of wasted time, was in the region of £5 billion.[1] The European Commission proposes a figure of €10 billion per year as the cost of spam to Internet users worldwide.[2] With regard to volume, Ian Lloyd notes that some 3.4 trillion e-mails were sent in the U.S. in 1998.[3] Of these, 2.7 trillion were commercial in nature, 96% of which could be regarded as spam.[4] Brightmail, a spam-filter company, has noted a recent sharp rise in the volume of spam being sent, estimating a 100% increase in the first half of 2002.[5] This trend accords with the findings of Jupiter Media Matrix, an Internet-based market researcher, who predict that 206 billion unsolicited commercial e-mails will be sent in the U.S. in 2006—this figure corresponds to 1,400 junk e-mails per Internet user, compared to 700 this year.[6]

The most striking aspect of these statistics is the staggering volume of unsolicited commercial e-mail being disseminated annually and there follows the additional issue of being able to calculate the size of the problem in hand. In this regard, most parties affected by the problem of junk e-mail have adopted the pragmatic mindset of concentrating their efforts on the control of the problem, rather than undertaking the near-impossible task of calculating the exact cost of it, an approach which will be followed throughout this Article. Perhaps a greater problem which emerges from the above statistics is that of the classification and definition of spam e-mail. Wye-Keen Khong[7] notes that the utopian definition of spam will include all e-

1. James Glave, *Novell Spam Report Boomerangs*, WIRED NEWS, Apr. 29, 1998, *available at* http://www.wired.com/news/print/0,1294,11994,00.html.

2. EUROPEAN COMMISSION, COMMISSION STUDY: JUNK E-MAIL COSTS INTERNET USERS EURO 10 BILLION A YEAR WORLDWIDE 9 (2001), *available at* http://europa.eu.int/comm/internal_market/en/dataprot/studies/spam.htm.

3. IAN J. LLOYD, INFORMATION TECHNOLOGY LAW § 28.13 (3d ed. 2000).

4. As a point of comparison, the U.S. Postal Service delivered 107 billion letters and parcels in the same year. *Id.*

5. Jane Black, *Special Report: The E-Mail Monster: The High Price of Spam*, BUSINESS WEEK ONLINE, Mar. 1, 2002, *at* http://www.businessweek.com/technology/content/mar2002/tc2002031_8613.htm?tc.

6. Charlie Taylor, *Can the Spam*, NUA, Mar. 25, 2002, *at* http://www.nua.ie/surveys/analysis/weekly_editorial/archives/issues1no219.html.

7. Wye-Keen Khong, Regulating Spams on the Internet, *in* 15th BILETA Conference: Electronic Datasets and Access to Legal Information, Apr. 14, 2000 (transcript available at http://www.bileta.ac.uk/00papers/khong.html).

mails which are of no benefit to the recipient from the point of view of the recipient. But this quickly becomes problematic when looked at in practical terms. The first barrier that can be identified occurs when one attempts to control 'unsolicited *bulk* e-mail' as has been attempted in Australia.[8] By classifying spam as all e-mail that is both unsolicited and bulk in nature, restrictive regulation is likely to conflict with the rights of citizens' free speech, where the e-mail in question is not commercial in nature. As will be seen below, this has caused legal difficulties for anti-spam legislation in the U.S., where the degree of constitutional protection for commercial speech is lower than that for political speech. Khong also notes that definitional problems subsist when the term "unsolicited commercial e-mail" is applied.[9] He correctly notes that different jurisdictions may apply widely different interpretations to the term "commercial."[10] The problem is particularly acute when attempting to define traditionally public services, such as education or health care, which may have been semi-privatized and for which a fee is paid.

One major concern of legislators within the European Union is that the negative publicity surrounding unsolicited commercial e-mail will impinge directly upon the legitimate activities of bona fide online commercial enterprises. M.Y. Schaub has argued that, in time, the direct e-mail marketing to previous customers by online businesses may become a widely accepted marketing tool, on the premise that if a consumer has obtained goods or services from a particular retailer, he may be interested to hear of future offers of similar goods or services from the same company.[11] Further problems emerge when online purchases give rise to the divulging of the consumer's e-mail address to third-party companies, who may or may not use the address for legitimate commercial purposes.

Given all these problems, the author proposes the following definition. Taken from a report on Electronic Mailing and Data Protection, the Commission Nationale de L'Informatique et des Libertés, an independent French commission, defines spam as:

> The practice of sending unsolicited e-mails, most frequently of a commercial nature, in large numbers and repeatedly to individuals

8. Definitions of Words We Use, Coalition Against Unsolicited Bulk E-mail, Australia, Web site, *at* http://www.caube.org.au/whatis.htm (last visited Feb. 9, 2003) (defining UBE).

9. Khong, *supra* note 7.

10. *Id.*

11. M. Y. Schaub, *Unsolicited Email: Does Europe Allow Spam? The State of the Art of the European Legislation with Regard to Unsolicited Commercial Communications*, 18 COMPUTER L. & SEC. REP. 99 (2002).

> with whom the sender has no precious contact, and whose e-mail address may be found in a public place on the Internet, such as newsgroups, mailing lists, directory or website.[12]

Following a brief history of spam and a discussion of the problems it creates and of those who are affected, this Article proposes to trace the origins of the law with regard to spam, to assess its merits, and to discuss what may occur in the future. While the perspective will be that of a researcher from Europe, where the discussion on spam has been thrown open once more in light of the proposed Electronic Communications Privacy Directive,[13] due attention will be paid to the laws of the U.S., where the majority of the world's spam originates, as well as to other international jurisdictions. Due to the fact that spammers are generally unable to ascertain the geographical whereabouts of their audience, the state of the law in the U.S. is therefore of global relevance. In this light, the efforts of various international organizations to co-ordinate the laws of national and supra-national legislatures will also be discussed. Various legal approaches will be considered, including the common law, legislation and self-regulation as well as the non-legal, technical solutions which are becoming more prevalent today.

II. UNSOLICITED COMMERCIAL E-MAIL

A. A Brief History

The precise manner in which the term spam came into current usage has become a great source of debate amongst hardcore Internet geeks and hackers. The term probably originated in the mid-1980's following an incident in which a MU.S.H (multi-user shared hallucination)[14] user caused technical difficulties by creating a macro which repeatedly typed the word "SPAM."[15] The prankster may have been inspired by a Monty Python comedy sketch that takes place in a restaurant where every meal on the menu contains spam, an unpalatable tinned meat product for which Hormel Foods owns the

12. Commission Nationale de l'Informatique et des Libertés, Report of October 14, 1999, *available at* http://www.cnil.fr.

13. Commission Proposal for a Council Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (C113E) 39 [hereinafter Commission Proposal on Protection of Privacy].

14. A MU.S.H is a type of MUD (multi-user dimension). David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 325 n.2 (2001).

15. *Id.*

U.S. trademark,[16] and to which some commentators directly link current usage of the word.[17] In any case, the term spam came to be applied to articles posted to Usenet newsgroups which were of no relevance to the discussion involved and which violated forum policies and rules of custom.[18] Such articles were often cross-posted to many newsgroups and quickly became a nuisance—so much so that at one point, the number of genuine articles were outnumbered by spam messages.[19] Gradually, the term spam became used to describe junk e-mail messages, generally advertisements for products and services of a dubious nature. Although the term has been applied to unwanted telephone[20] and fax[21] messages as well as to the repetition of words on a Web page to enhance the opportunity for retrieval by search engine,[22] the term spam is today synonymous with unsolicited commercial e-mail.

Coinciding with the rise in the use of the Internet as a commercial medium, the first instances of spamming occurred in 1993. A U.S. couple, Lawrence Canter and Martha Siegel, retain the dubious honor of being the first large-scale spammers.[23] Their advertisement, publicizing a green card employment scheme, was posted to thousands of newsgroups within a short space of time. The public reaction was swift and decisive. Users began to mail bomb the couple's e-mail address, causing their mailbox to overload and probably preventing any genuine potential clients from contacting the couple.[24] Other users complained to the network service provider involved while other, more technically-minded netizens attempted to create a piece of software capable of automatically identifying and deleting the advertisements. Whatever the individual retaliatory approaches taken, the message from Internet users was clear: any

16. Spam Web site, *at* http://www.spam.com (last visited Feb. 8, 2003).

17. *See* David T. Bartels, *Review of Selected 1998 California Legislation: Canning Spam: California Bans Unsolicited Commercial E-mail*, 30 MCGEORGE L. REV. 420, 420 n.1 (1999).

18. Lloyd L. Rich, *Internet Legal Issues: SPAM,* PUBLISHING LAW CENTRE, 1999, *available at* http://www.publaw.com/spam.html (last visited Feb. 9, 2003).

19. LLOYD, *supra* note 3, § 28.14.

20. B. Foss, *Blasts Filling Voice Mail: A Nuisance, or an Efficient Way to Communicate?*, CHI. TRIB., Oct. 11, 1999.

21. Drew Cullen, *LA Citizens Tackle NFL in Mass Fax Spam*, THE REGISTER, Aug. 25, 1999, *at* http://wwwthergister.co.uk/content/archive/6369.html.

22. Ira S. Nathenson, *Internet Infoglut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 HARV. J.L. & TECH. 43, 46–47 (1998).

23. Khong, *supra* note 7.

24. *Id.*

breach of behavioral norms on the Internet (known colloquially as "netiquette")[25] would result in punishment. The development of this vigilante regulation into a more sophisticated body of law will be discussed later in this section. Beforehand, the primary issue of the type of damage caused by unsolicited commercial e-mail, as well as the main parties affected, will be addressed.

B. Problems with Unsolicited Commercial E-Mail

At the heart of this issue lies a contradiction. In attempting to strike a balance between the rights of commercial entrepreneurs to market their wares and the rights of e-mail users to be free from unwarranted solicitation, a clear contradiction exists between business interests and those of private individuals.[26] Although it would appear difficult as to where to draw the line in this regard, it seems that instances of e-mail users receiving upwards of four spams for every one legitimate e-mail[27] should tip the balance in favor of the protection of the individual. The main problem with unsolicited commercial e-mail and the reason for its proliferation is the shifting of the costs involved away from the advertiser onto the consumer and other parties. Unlike passive forms of advertising, such as television commercials or billboards, direct marketing usually involves some degree of effort or involvement on the part of the consumer. However, unlike door to door sales or other cheaper forms of direct marketing, such as telephone and fax solicitation, the cost of sending an e-mail is negligible and does not rise in proportion to the number of solicitations made.[28] This fact has enabled, even encouraged, marketers to send out as many copies of their e-mail as possible, a figure often running into the millions. Internet users incur the costs of these e-mails by spending time online sifting through, identifying, and deleting the messages and may also incur further costs in attempting to unsubscribe from the marketers' mailing lists. If, as was the case for the unfortunate plaintiff in *Parker v. C.N. Enterprises*, the spammer elected to forge a return e-mail address which corresponds to that of an unsuspecting Internet user or server, that person will

25. Memorandum from Sally Hambridge, Network Working Group, to the Internet Community on Netiquette Guidelines (Oct. 1995), *available at* http://www.ietf.org/rfc/rfc1855.txt (last visited Feb. 10, 2003).

26. Schaub, *supra* note 11.

27. P. Freeman, *Telecom Issues Top Consumer Complaints*, PUGET SOUND BUS. J., Oct. 2, 1998, at 26.

28. Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 364 (2000).

receive all of the returned mail which had been sent to incorrect addresses.[29] In *Parker*, the number of returned messages numbered tens of thousands.[30]

Apart from the end consumer, the other major victims are the Internet service providers (ISPs) who process the e-mails. Servers quickly become clogged when inundated with the large volume of mail associated with spams—massive amounts of bandwidth and memory are consumed and associated administrative costs are incurred.[31] Although ISPs may suffer a loss of business and, indeed, reputation due to continued clogged bandwidth as a result of relaying spam, the costs in increasing bandwidth to deal with spam will simply be passed on to the consumer in the form of higher access fees. This problem has become so acute that some Web sites are beginning to discontinue free e-mail services. David Sorkin argues that if spam continues to increase exponentially in years to come, the increase in cost could lead to the demise of e-mail as the near-universal communication method it is today.[32]

Aside from the issue of volume, consumers often take exception to the content of spam advertisements. As noted above, the goods or services offered for sale are frequently of a dubious nature[33] and often involve pornography or get-rich-quick pyramid schemes.[34] It is not hard to imagine the offense that these often borderline legal messages may cause to many Internet users, and the fact that sexually explicit material may be sent to minors and children is a cause of alarm for many parents. A broader sociological issue raised by this phenomenon, and one addressed briefly by Tibor Beke, is the question as to how this type of advertising has become so prevalent on a medium where the level of income and education of its users has been shown to be higher than the median.[35] Another problem with

29. Parker v. C.N. Enter., No. 97-06273 (D. Tex. 1997).

30. DENIS KELLEHER & KAREN MURRAY, IT LAW IN THE EUROPEAN UNION § 9.27 (1999).

31. Khong, *supra* note 7.

32. Sorkin, *supra* note 14, at 338–39.

33. A recent humorous article in the Onion poked fun at the general content nature of spam advertisements. *See generally Anti-Spam Legislation Opposed by Powerful Penis-Enlargement Lobby*, THE ONION, July 17, 2002.

34. The author has been the recipient of numerous junk mails which begin with the words THIS IS NOT A PYRAMID SCHEME and which go on to describe in depth the operation of a classic pyramid scheme, illegal in many jurisdictions.

35. Tibor Beke, *Fending Off Automated Mass Electronic Mail: or, How to Distinguish Yourself from a Computer*, FIRST MONDAY (1998), *at* http://www.firstmonday.dk/issues/issue3_2/beke/ (last visited Feb. 10, 2003).

spam content arises when attached files are found to contain hostile viruses, such as occurred with the infamous Melissa Virus in 1999.[36] Looked at in this context, spam can also be categorized as a security threat.[37]

Different jurisdictions identify different problems with spam. An interesting perspective is the German one, not in the least given that country's influence in the European legislative sphere. N. Härting gives a good account of the development of German law on unsolicited commercial e-mail stemming from existing law on phone and fax marketing. As well as focusing on problems such as cost, time, and wasted effort, Härting identifies invasion of privacy, disruption of market relations, and the anti-competitive nature of free e-mail marketing as problems that legislation should address.[38] Indeed, Germany remains the only European country to have had a court ruling on the issue of spam.[39] The issue of privacy remains an interesting one. In an age where many citizens have dispensed with notions of familial and personal privacy,[40] it is interesting to reflect on the writings of modern German philosophers such as Jürgen Habermas,[41] who recognize the existence of a private sphere of life, as distinct from the collective interests of the public sphere, today manifested by digital mass communication media such as the Internet.[42]

All of these factors taken together and compounded by the proliferation of ISPs, Internet cafes, (where the user has no direct contract with a service provider and thus can retain anonymity)[43] and

36. For a good article on the Melissa Virus, see the Web page of the Carnegie Mellon University Software Engineering Institute. Carnegie Mellon University Software Engineering Institute, Frequently Asked Questions about the Melissa Virus, *at* www.cert.org/tech_tips/Melissa_FAQ.html (last visited Feb. 10, 2003).

37. Sorkin, *supra* note 14, at 336.

38. N. Härting, Internet Recht, Verlog Dr. Otto Schmidt, Köln (1999).

39. Beschluß des Landgerichts Traunstein [trial court], 2HK O 3755/97 (Oct. 14, 1997). The decision will be discussed in Part IV.

40. Diane Rowland, Anonymity, Privacy and Cyberspace, *in* 15th BILETA Conference: Electronic Datasets and Access to Legal Information (2000), *available at* http://www.bileta.ac.uk/00papers/rowland.html (last visited Feb. 10, 2003).

41. *See* JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY, (Thomas Burger trans., 1989) (1962).

42. For a good article on privacy and the law in cyberspace, see Debra A. Valentine, General Counsel, Federal Trade Commission, *Privacy on the Internet: The Evolving Legal Landscape*, Prepared Remarks at Before Santa Clara University (February 11–12, 2000) (transcript available at http://www.ftc.gov/speeches/other/dvsantaclaraspeech.htm).

43. LLOYD, *supra* note 3, at § 28.16.

mail relay servers amount to quite a sizeable problem. The additional effects of spam have served to disrupt mainstream e-commerce and other businesses to an incalculable degree. Reports even indicate that certain U.S. Internet service providers and systems administrators have been banning all unknown e-mail from large portions of Asia, where it is believed that unregulated servers are being used to relay spam to the U.S.[44] The effects of this type of move serve only to shatter confidence in the e-commerce sector and point to the need for an over-arching legal framework as the only solution to the problem. As Gary Moorefield puts it, "[t]he question is not whether the medium of UCE [Unsolicited Commercial E-mail] messages serves some good; the question is whether the drawbacks of this medium of commercial expression outweigh the benefits to a degree that necessitates government intervention and control."[45]

The stark need for government control becomes only clearer when one examines the piecemeal and unaccountable self-regulatory procedures that sprang up to deal with the problem of spam when it first presented itself.

C. The Move Away From Self-Regulation

As mentioned above, the first major cases of spamming, such as the Canter and Siegel episode, aroused the wrath of Internet users who used various techniques to retaliate to the unwarranted interference with their Web space. Most popular amongst these was the use of mail bombs—computer programs capable of sending and re-sending many thousands of e-mails to a particular account, usually clogging it.[46] Complaints were also made to the spammer's ISP and this usually resulted in the expulsion of the spammer. The spammers themselves, however, quickly became more sophisticated and began to forge false return addresses in their e-mail headers,[47] with the result that any attempts to retaliate would lead to the clogging of an innocent user's account or even the crippling of a small ISP. For this reason, the vigilante response is described by Michael Fisher as a

44. Mark Webber, *Spam Flood Prompts New Barriers,* WORLD EBUSINESS LAW REPORT, Apr. 11, 2002, *available at* http://www.cptech.org/ecom/spam/spam-flood2.html.

45. Gary S. Moorefield, *SPAM—It's Not Just for Breakfast Anymore: Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-mail*, 5 B.U. J. SCI. & TECH. L. 10, 10 (1999).

46. Fisher, *supra* note 28, at 399.

47. S*ee* Ken Lucke, *Reading Email Headers* (1997), *at* http://www.stopspam.org/email/headers/headers.html (last visited Feb. 10, 2003) for an excellent general introduction to e-mail headers.

"blunt and inaccurate tool."[48] Aside from individual retaliatory methods, anti-spam groups have been established with the aim of stigmatizing spammers into submission. Groups such as the Coalition Against Unsolicited Commercial E-Mail (CAUCE),[49] Junkbusters[50] and the Mail Abuse Prevention System (MAPS)[51] offer users legal and technical advice on how to combat spam and engage in lobbying activities. MAPS maintains what it terms the "Realtime Blackhole List," a blacklist of servers that are *not* anti-spam and which are available to other ISPs so that they may block mail from these networks.[52] This practice raises a number of problems. Firstly, the MAPS blacklist is based on a definition of spam (involving the lack of a double opt-in system) that MAPS itself produced. This means that conscientious e-mail marketers who honor single opt-in or even opt-out schemes, will nonetheless be blacklisted under MAPS' terms. Another problem with this type of blacklist is that if one user sends spam from an ISP, all users from the same ISP will be blacklisted, with the consequence that much legitimate e-mail is blocked.[53] A further problem with blacklists and the self-help response to spam in general is the lack of accountability involved and the fact that such systems are widely open to abuse. For instance, one could imagine the ease with which a political rival or a commercial competitor could anonymously or by pseudonym denounce a particular individual or company as a spammer, thus removing that person's ability to communicate via e-mail.[54] When one considers what is at stake—the right to communicate or trade—it is not surprising that many commentators balk at the notion of such regulation being enforced by a faceless, private Internet company, with no right of recourse or

48. Fisher, *supra* note 28, at 400.

49. *See* http://www.cauce.org (last visited Feb. 10, 2003); EuroCAUCE, *at* http://www.euro.cauce.org/ (last visited Feb. 10, 2003).

50. *See* http://www.junkbusters.com (last visited Feb. 10, 2003).

51. *See* http://mail-abuse.org/ (last visited Feb. 10, 2003).

52. *See* http://mail-abuse.org/rbl/ (last visited Mar. 31, 2003).

53. Sabra-Anne Kelin, *State Regulation of Unsolicited Commercial E-Mail*, 16 BERKELEY TECH. L.J. 435, 442–43 (2001).

54. PC World.com has reported a recently filed case in this regard. Mark Turner, president of e-mail advertising firm Opt-In Marketing Services has filed suit against his ISP and three anti-spam organizations, claiming that the anti-spam groups are 'sinister entities' who have conspired to put him out of business by faking complaints about his activities. He also claimed that such organizations have, in the past, accepted donations from AOL and MSN in return for turning a blind eye to those large ISPs' efforts to send their own unsolicited commercial e-mail. Daniel Tynan, *Spammers Claim Rights, Too: Opt-In Marketing Services Challenges Anti-Spam Efforts, Organizations in Court*, PCWORLD.COM, June 3, 2002, *at* http://www.pcworld.com/news/article/0,aid,101610,00.asp.

public involvement.[55]

Gahtan et al. provide a practical list of actions that private individuals may have recourse to in order to prevent spam and to assist those who do receive junk mail.[56] Actions such as ensuring that their ISP is not using background programs that enable Web servers to harvest e-mail addresses, not disclosing their address in public areas, using spam filtering software, and forwarding spam to the ISP of both recipient and sender are all useful and pragmatic approaches.[57] However, they do little in the way of stemming the spam tide or, indeed, discouraging the junk mail from being sent in the first instance. Attempts to discourage the sending of spam by stigmatizing it have only been successful to a certain degree. As Sorkin notes, such attempts have only served to make bulk mailing a fringe activity—this is undoubtedly a major reason for the dubious moral quality of many of the goods and services advertised through spam—and social pressures tend to be largely ineffectual against such groups.[58]

Attempts by ISPs to self-regulate their industry have been equally hampered. The simplest method with which an ISP can regulate spam is through an appropriate clause in its contractual use policy. Most ISP license agreements contain a clause banning the sending of bulk mail outright through its network. There are several reasons why such licenses are largely ineffective against spammers but the main problem is that of enforceability. According to Hoffman & Crocker, these legally binding agreements lack enforceability due to the difficulty in reliably identifying the originators of junk mail.[59] Another factor has been the difficulty in proving a precise level of damage but, as will be examined later, this issue has not deterred ISPs from initiating litigation. Another legal stumbling block for ISPs in this regard has manifested itself in relation to the blocking of incoming spam. Although measures taken to block the sending of spam have the force of contract law, in the case of incoming spam the sender has no contract with the recipient's ISP. This leaves the receiving ISP powerless to deal with junk mail until after it has been

55. *See, e.g.*, Kelin, *supra* note 53, at 441–43; Sorkin, *supra* note 14.

56. ALAN M. GAHTAN, MARTIN P. J. KRATZ, & J. FRASER MANN, INTERNET LAW: A PRACTICAL GUIDE FOR LEGAL & BUSINESS PROFESSIONALS 178–80 (1998).

57. *Id.*

58. Sorkin, *supra* note 14, at 341–44.

59. Paul Hoffman & Dave Crocker, Internet Mail Consortium Report: UBE-SOL IMCR-008, Unsolicited Bulk Email: Mechanisms for Control, May 4, 1998, §6, http://www.imc.org/ube-sol.html.

sent. At this point, the ISP can act by dealing with the spam in either of two ways. Filtering software can be used to automatically delete any detected bulk mail, but this may lead to the elimination of genuine bulk or commercial mail. Secondly, bulk mail may be diverted to a special "bulk mail folder"[60] from where the recipient can choose whether to read or delete it. However, many critics argue that by this stage the damage has already been done.[61] Even if ISP contractual use policies were potent legal instruments, other problems emerge. For instance, Sabra-Anne Kelin notes that different ISPs have different use policies, which may in fact conflict, and that the resulting conflict of obligations could raise compliance problems not only for spammers, but also for other legitimate e-mail user groups.[62]

Problems, such as described above, have led ISPs (in the United States in particular) to investigate the possibility of forming trade associations to standardize business practices on the Internet which, through private contracts, could implement and enforce an industry-wide policy against junk e-mailing.[63] However, as Fisher points out, such a move, due to its collaborative nature could easily be used to suppress competition and would likely run afoul of federal antitrust laws, in particular section 1 of the Sherman Act.[64] Antitrust legislation in the United States is particularly stringent, as in the decision of the Supreme Court in *Fashion Originators' Guild of America, Inc. v. Federal Trade Commission*.[65] In reinforcing this point, the court found that an industry group boycott could not be justified on the basis of deterring tortious conduct.[66] On the other side of the fence, the International Federation of Direct Marketing Agencies (FEDMA)[67] launched an e-mail preference service initiative in 1998 in an attempt to curb the growing clamor surrounding the practice of unsolicited commercial and bulk e-mailing, a practice that FEDMA believed to be a highly useful marketing tool if used responsibly. Basically, the e-mail preference service, the U.K.

60. In the UK, this service was pioneered by Yahoo! UK in December 1999 and is offered by most major e-mail providers in some shape or form today.

61. Sorkin, *supra* note 14, at 345–46.

62. Kelin, *supra* note 53, at 441–42.

63. David A. Gottardo, *Commercialism and the Downfall of Internet Self Governance: An Application of Antitrust Law*, 16 J. MARSHALL J. COMPUTER & INFO. L. 125, 141–42 (1997).

64. Fisher, *supra* note 28, at 396 (citing the Sherman Antitrust Act, 15 U.S.C. § 1).

65. Fashion Originators' Guild of Am., Inc. v. Fed. Trade Comm'n, 312 U.S. 457 (1941).

66. *Id.*

67. *See* Preferences Services in Europe, FEDMA Web site, *at* http://www.fedma.org/code/page.cfm?id_page=77# (last visited Mar. 31, 2003).

version of which was launched in January 2000 by the UK Direct Marketing Association,[68] is a large spam opt-out register maintained by the DMA and supposedly consulted regularly by advertisers who are members of the DMA. In its first years of use in the U.K., the register has proved a resounding failure. It is highly unlikely that the register is consulted by more than a handful of spammers—certainly not by those to whom it was intended to apply—and consequently, its usefulness in the future is very much in doubt.

For all the reasons mentioned above, the various forms of vigilante, self-help, and industry regulation applied to the problem of unsolicited e-mail advertising have been of limited practical use. These shortcomings and the growth of the spam problem to epidemic proportions lead to the need for urgent government control. Other private actors have taken their own action in the form of litigation and the resulting body of emerging substantive law will be examined in the next two parts.

III. UNSOLICITED COMMERCIAL E-MAIL LAW IN THE U.S.

A. The Emergence of Substantive Law

As previously mentioned, the U.S. approach toward the law governing unsolicited commercial e-mail is important for a European perspective on this issue for a number of reasons. First, the majority of bulk e-mail advertisement received by European e-mail users originate in the U.S. and are intended for a U.S. audience. Such e-mails are of no relevance to European consumers and can thus be easily classified as junk e-mail. Although European e-mail users therefore remain passive actors in this regard, those who find themselves in receipt of burdensome quantities of U.S. junk mail may have more than a passing interest in what is being done in that jurisdiction to combat the problem. The issue of international jurisdiction and the future possibility of a global harmonization of e-commerce law will be discussed in Part V. Second, as the U.S. was the first country to encounter a major problem with spam and was also the first jurisdiction to attempt to deal with the problem on a legal basis, the law there today is in a more evolved state than anywhere else in the world. Lessons may thus be learned from the U.S. experience, the approach taken and the mistakes made. A third

68. Advert. Info. Group, Notice No. 75, UK: DMA Launches E-Mail Preference, Jan. 18, 2000 at 4–5.

pertinent reason to examine the U.S. legal framework is due to the jurisprudential similarities between that country and the UK. As a common law country, decisions of U.S. court, though not of binding authority in the UK and Ireland, will be of persuasive authority and so parallels may be drawn between common law actions taken against spammers there and possible future actions in this jurisdiction. With respect to European Union legislative measures, certain parallels may also be drawn between the federal-state dichotomy in the U.S. and the increasingly conspicuous federalist nature of EU law. This is particularly evident when it comes to laws relating to the emerging digital technologies and the information society, a field in which the EU clearly aspires to become a world leader. A further point of reference between the two legal backdrops is the starting point for the development of a law against spam, that of analogy with the law in relation to commercial telephone and fax solicitations.

The history of U.S. law on junk mail, telephone and fax advertising is an involved and complicated one[69] which the author will not burden the reader with in these pages, but a brief synopsis is of benefit. In *Rowan v. United States Post Office Department*,[70] the Supreme Court was invited to consider the constitutionality of legislation[71] that provided consumers with a means for removing their names and addresses from the postal mailing lists of marketers who were publicizing erotic or sexually provocative material. In rejecting the argument that the statute violated the plaintiff's right to communicate and in upholding the statute, the Court found that "nothing in the Constitution compels [people] to listen to or view any unwanted communication, whatever its merit."[72] The crucial aspect of Title III of the Postal Revenue and Federal Salary Act of 1967 was that it vested power in the private homeowner, rather than the government, to regulate what mail he did or did not receive:

> Congress provided this sweeping power not only to protect privacy but to avoid possible constitutional questions that might arise from vesting the power to make any discretionary evaluation of the

69. For good, in-depth articles on the subject see Jonathan Byrne, *Squeezing Spam off the Net: Federal Regulation of Unsolicited Commercial E-mail*, 2 W. VA. J. L. & TECH. 1.4 (1998), *at* http://www.wvu.edu/~wvjolt/Arch/Byrne/Byrne.htm; Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L. J. 233 (1996).

70. Rowan v. United States Post Office Department, 397 U.S. 728 (1970).

71. Title III of the Postal Revenue and Federal Salary Act of 1967, 39 U.S.C. § 4009 (1964 ed., Supp. IV) (current version at 39 U.S.C. § 3010 (2000)).

72. *Rowan*, 397 U.S. at 737.

material in a government official.[73]

Commercial telephone and fax solicitations may be regarded as even more analogous to e-mail spamming. Such activities were legislated against by the Telephone Consumer Protection Act of 1991 (TCPA).[74] The TCPA prohibits the use of auto-dialers to play pre-recorded messages to homes and businesses and also forbids the sending of unsolicited commercial solicitations from computers or fax machines to telephones or fax machines. The Act encountered almost immediate constitutional challenge in *Destination Ventures v. Federal Communications Commission*,[75] where it was upheld both at first instance and on appeal. Both courts found that Congress had a substantial interest in a very real problem; unsolicited faxes were an invasion of privacy, a waste of valuable business time and opportunity and, above all, represented an unacceptable shifting of the costs (in terms of ink and toner) to the recipient.[76] Moorefield comments that the decision in *Destination Ventures* not only simply validated the TCPA but also went further, paving the way for the expansive interpretation of the Act to include unsolicited commercial e-mail.[77] An analogous argument was put forward by the plaintiff in the case of *Snow v. Doherty*[78] but, as Jan Samoriski[79] points out, a detailed reading of the TCPA leaves little doubt that the legislature intended the Act to apply solely to transmissions by fax. There are good reasons for not extending the reach of the TCPA to cover spam (due to the inherent nature of e-mail technology) and such will be touched upon in the discussion on U.S. legislative measures. Therefore, by the mid-1990's as spam became an increasingly problematic phenomenon, there was a void of legislation on the issue. Although there was some political discussion on the subject,[80] ISPs

73. *Id.* at 743.

74. 47 U.S.C. § 227 (1994).

75. Destination Ventures v. Fed. Communications Comm'n, 844 F. Supp. 632 (D. Or. 1994), *aff'd*, 46 F.3d 54 (9th Cir. 1995).

76. Moorefield, *supra* note 45.

77. *Id.*

78. *Snow v. Doherty*, No. 3:97-CV—0635 (RM) (N.D. Ind. 1997), *available at* http://mama.indstate.edu/users/dougie/lawsuit.html.

79. *See* Jan H. Samoriski, *Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?*, 43 J. BROAD. & ELEC. MEDIA 670 (1999).

80. *See, e.g.*, three federal bills proposed in 1997: Netizens Protection Act, H.R. 1748, 105th Cong. (proposed by Rep. Christopher Smith); Electronic Mailbox Protection Act, S. 875, 105th Cong. (Sen. Robert Torricelli); Unsolicited Commercial Electronic Mail Choice Act, S. 771, 105th Cong. (Sen. Frank Murkowski).

who were losing irate customers, business reputation, and countless dollars due to spamming decided to act first and instigate litigation against known spammers.

An early such case, and one which establishes important precedent is that of *CompuServe v. Cyber Promotions*.[81] The facts of this case were that the plaintiff, one of the largest ISPs in the U.S., ordered the defendant to cease using its network for the purpose of mass electronic mailings after the plaintiff CompuServe had received a flood of complaints from subscribers about the unacceptable volume of spam they were receiving.[82] Despite the plaintiff's request, and the fact that CompuServe expressly prohibited spamming through its acceptable use policy, the volume of spam being disseminated by Cyber Promotions increased. The plaintiff responded by introducing spam-filtering software that could automatically detect and delete mass mailings from the defendant. However, Cyber Promotions then began to falsify the sender information in the headers of its messages and to configure its server to falsify its domain name and IP address. Such manipulative behavior enabled the defendant to continue with its spamming activities and CompuServe felt it had no choice but to litigate, doing so on the basis of the common law theory of trespass to personal property (or chattels). Judge Graham in his judgment notes that "a trespass to chattel may be committed by intentionally using or intermeddling with the chattel in possession of another."[83] "Intermeddling" is defined as "intentionally bringing about a physical contact with the chattel."[84]

The judge goes on to cite authority for the assertion that electronic signals generated and sent by computer are sufficiently physically tangible to support a trespass cause of action,[85] and held that the defendant's contact with the plaintiff's computers was clearly intentional. Regarding the issue of damage (the tort of trespass to chattel in U.S. law requires some actual damage as a *prima facie* element, whereas damage is assumed where there is a trespass to real property), Judge Graham found that the diminished value of CompuServe's computer equipment, due to the defendant's "multitudinous electronic mailings" and the consequent draining of

81. CompuServe v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997).

82. *Id.* at 1017.

83. *Id.* at 1021 (citing RESTATEMENT (SECOND) OF TORTS § 217(b) (1965)).

84. *Id.* (citing RESTATEMENT (SECOND) OF TORTS § 217 cmt. e (1965)).

85. *Id.* (citing *Thrifty-Tel, Inc. v. Bezeneck*, 46 Cal. App. 4th 1559, 1567 (1996); *State v. McGraw*, 480 N.E. 2d 552, 554 (Ind. 1985); *State v. Riley*, 846 P.2d 1365 (1993)).

disk space and processing power was sufficient damage to uphold the course of action.[86] Further, the fact that CompuServe's full resources were unavailable to serve its subscribers, and the fact that many terminated their accounts, also meant that Cyber Promotion's intrusions were actionable as they harmed the plaintiff's goodwill and business reputation.[87] Judge Graham paid little credence to the defendant's claim to freedom of speech and ordered a preliminary injunction enjoining the defendant from sending any unsolicited e-mail to CompuServe subscribers.[88]

The *CompuServe* decision is an interesting one and, at first glance, appears to be a potent legal weapon against spammers, particularly as it was followed in *America Online v. IMS*[89] by a District Court in Virginia. But there are a couple of good reasons why the trespass to chattel cause of action may be of more limited application. First, one can gather from the facts of the case that this was an instance of what may be termed "aggravated spamming" i.e. the defendant was repeatedly ordered to cease and desist and yet continued with his course of action and even used evasive techniques in his efforts to continue. Although the *CompuServe* trespass doctrine may be readily applied to bulk mailers who have actual notice that they are trespassing, such a cause of action would be useless against a one time spammer or an individual using different accounts or network providers for each unsolicited advertisement sent. The second issue is one of enforcement. Back in 1997 it may have been relatively easy to track down a spammer, but the technical proficiency of today's mass e-mailers means that they are harder to locate. They are also often one-man operations unlike Cyber Promotions[90] which was, in fact, an identifiable and fully incorporated company. For these reasons, ISPs and other injured parties have had to seek out other legal doctrines on which to base their claims against spammers.

B. Litigating Against Spammers: Causes of Action

As Dianne Latham rightly points out, "[t]he list of potential offenses spammers commit is extensive . . . . . .[t]racking down spammers in cyberspace is more difficult than finding legal theories

86. *CompuServe*, 962 F. Supp. at 1022.
87. *Id.*
88. *Id.*
89. Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E. D. Va. 1998).
90. See *CompuServe*, 962 F. Supp. 1015.

under which to charge them."[91] The practice of using false return addresses in e-mail headers and the increasing use of forgery by spammers where mass mailers forge the name of a well-respected company into the subject line or body of their advertisement both to evade filters and to increase the legitimacy of the e-mail greatly increases the number of potential causes of action against them. Consequently, different legal approaches are adapted to best suit the facts of any given case. While examining the various legal theories it is worth keeping in mind the aforementioned quote by Latham and the fact that, in very many cases, simply tracking down and identifying the spammer may prove the most difficult obstacle in spam litigation.

The two cases mentioned in the previous subsection, those of *CompuServe v. Cyber Promotions* and *AOL v. IMS*, both involved a large ISP suing a spammer for trespass to chattel. However, the first spam related suit was a small claims case taken by an individual e-mail subscriber, Robert Arkow, against CompuServe in 1995.[92] The claim, based on the expansive interpretation of the Telephone Consumer Protection Act of 1991 and which was settled out of court for undisclosed terms,[93] raises the issue of the right of individual subscribers to sue spammers directly. Fisher proposes that a trespass cause of action could be available to private e-mail users, who have a proprietary interest in their e-mail account.[94] However, issues such as the difficulty of proving actual harm,[95] to show accumulation of any injury, and the prohibitive costs involved in going to court may limit the effectiveness of this remedy. Class actions are pointed out as a possible solution to these problems.[96] However, other, particularly evidentiary, problems emerge and in the absence of specifically tailored legislation, such an action would likely fail.

Other than a trespass claim, the next, most common action against spammers is trademark infringement and false designation of origin. False designation of origin is a violation of 15 U.S.C. § 1125

91. Dianne Plunkett Latham, *Electronic Commerce in the 21st Century: Article, Spam Remedies*, 27 WM. MITCHELL L. REV. 1649, 1651 (2001).

92. David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, n.12 (1997).

93. *Id.*

94. Fisher, *supra* note 28, at 387.

95. Anne E. Hawley, Comment, *Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising Via Electronic Mail*, 66 UMKC L. REV. 381, 403 (1997).

96. Fisher, *supra* note 28, at 388.

(a)(1) of the Lanham Act. In *America Online v. IMS,*[97] the defendant was caught by this subsection as he falsely designated the origin of his e-mail as coming from AOL and in doing so had deceived recipients and had caused damage. The Court applied a three-pronged test: (1) The alleged violator must employ a false designation; (2) the false designation must deceive as to origin, ownership or sponsorship; and (3) the plaintiff must believe that he or she is or is likely to be damaged by such an act.[98]

In a similar case involving the same plaintiff and almost identical facts, *America Online v. LCGM*, the court applied a slightly different test with the same effect.[99] A false designation of origin claim is supported if:

> (1) a defendant uses a designation; (2) in interstate commerce; (3) in connection with goods and services; (4) which designation is likely to cause confusion, mistake or deception as to origin, sponsorship, or approval of defendant's goods or services; and (5) plaintiff has been or is likely to be damaged by these acts.[100]

Also falling within the ambit of the Lanham Act is trademark dilution.[101] Raised successfully in *IMS* and *LCGM*, dilution entails the reduction of the distinctive quality of a famous or well-known service mark. The dilution claims in the *AOL* decisions were based on the doctrine of "tarnishment," which requires evidence to the effect that the famous mark will be diminished through the negative association with the defendant's use. The *AOL* decisions seem to highlight the effectiveness of the trademark infringement approach in cases where the sender of spam has forged e-mail headers. Dilution claims are further strengthened by the fact that as Khong notes,[102] the U.S. courts have taken a dim view of the practice of spamming and that a negative association will be assumed for the purposes of a dilution claim under the tarnishment heading.

As was mentioned before, a breach of contract case may also be taken by an ISP against a spammer with whom contractual relations exist. A good example of such a case is *Hotmail Corp. v. Van$ Money Pie Inc*. There, the Northern District Court of California found the defendant to have breached the Hotmail subscriber service

97. *See* Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E. D. Va. 1998).
98. *Id.* at 551 (citing Lanham Act, 15 U.S.C. § 1125(a)(1)).
99. Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998).
100. *Id.* at 449 (citation omitted).
101. Lanham Act, 15 U.S.C. § 1125(c)(1) (2000).
102. Khong, *supra* note 7.

agreement by sending spam from a falsely designated Hotmail address and using a separate Hotmail account to return invalidly addressed messages which were never read.[103] The *Hotmail* case was a relatively straightforward application of the law of contract as the Hotmail service agreement specifically prohibited the sending of unsolicited bulk e-mail and made a provision for the termination of accounts whose users had violated the terms of service.[104] Such cases become more difficult where the service contract makes no specific reference to unsolicited bulk e-mail but provides for punitive action where a "breach of netiquette" or some other equally broad term occurs.

This very point was addressed, however by a Canadian Court, in the case of *1267623 Ontario Inc. v. Nexx Online Inc.*[105] Here, Nexx Online hosted the plaintiff's Web site from which the plaintiff sent unsolicited promotional e-mails to many Internet users who, in turn, complained to the defendant. The defendant responded by informing the plaintiff that such activity was in breach of its hosting agreement, which contained a term obliging signatories to follow generally accepted "netiquette" when sending e-mails or posting to newsgroups. This warning was not heeded however and the plaintiff then engaged a third party to send more spam promoting its business. This led the defendant to deactivate Ontario's Web site and reactivate the plaintiff's application for an interlocutory injunction. The Ontario Superior Court of Justice, in rejecting the plaintiff's application, held that the defendant was permitted to discontinue the hosting of the Web site as the plaintiff's conduct constituted a breach of the parties' contract.[106] In so holding, the court recognized that the practice of sending unsolicited bulk e-mail was contrary to the emerging principles of "netiquette." Furthermore, the court found that the plaintiff had breached another provision of the contract which permitted the defendant to add additional terms upon notice to the plaintiff. Examining the conduct of the parties, the court found that the defendant's warning to the plaintiff to cease its spamming activities constituted notice of the defendant's wish to add just such an additional term.[107] The case represents not only the power of private contract law to help ISPs combat the spam problem in cases

103. Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998).
104. *Id.* at 1025.
105. 1267623 Ontario, Inc. v. Nexx Online, Inc., 45 O.R.3d 40 (Ont. Sup. Ct. 1999).
106. *Id.* at 50.
107. *Id.*

where the spammer can be identified, but also is important in light of the court's recognition of the legally binding status of self-regulatory online norms such as netiquette. Although most ISP service agreements today contain specific provisions relating to spam, the decision of the Canadian Courts to recognize netiquette may have broader implications relating to the law in other areas of e-commerce, particularly if other jurisdictions choose to follow it.

The *Ontario* decision, as well as most of the aforementioned cases, represents instances where the injured party has sought equitable relief (usually in the form of an interlocutory or preliminary injunction) as opposed to monetary relief. Although the successful party in an application for injunctive relief will often be successful in obtaining an order for costs, significant damages are seldom awarded due to the difficulty in quantifying the precise loss to an ISP due to spamming.

Another hurdle in the way of pecuniary recompense for ISPs has been the issue of agency. The issue of agency arises when an advertiser, as in the *Ontario* case, engages an independent contractor to mount a spam campaign on his behalf. In such an instance, if the affected ISP wishes to, it could relatively easily obtain an injunction through a trespass, trademark or contract action against the advertiser; if he wishes to obtain damages, the preferred option would be to sue the advertiser directly, as the party would be more likely than an independent contractor to have sufficient capital to be able to afford such a payment. However, for this to succeed a plaintiff must be able to show that the damage caused by the spammer was carried out in the course of employment or under conditions whereby the spammer's actions were subject to the customer company's control, and thus the advertiser becomes vicariously liable. The hub of the issue boils down to the instructions that the advertiser gives to the 'agent,' whether the harm is done by some devilment dreamt up and carried out solely by the contractor, without the knowledge of the advertiser.[108] *Ontario v. Nexx Online* is a good example of the former, as the company in that case engaged a third party for the purposes of carrying out spamming activities of which it had notice were in breach of the service contract.

America Online, Inc. v. National Health Care Discount, Inc. (NHCD)[109] was a case brought by AOL for summary judgment

108. *See* Joseph D'Ambrosio, *Should Junk E-Mail be Legally Protected?*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 231, 238–39 (2001).

109. Am. Online, Inc. v. Nat'l Health Care Discount, Inc. (NHCD), 121 F. Supp. 2d 1255

against NHCD, relating to over 76 million unsolicited e-mails sent by the defendant. The District Court Judge ruled that the question of whether the contract e-mailers engaged by NHCD to carry out the campaign were acting as agents was a genuine issue of material fact that precluded the granting of a summary judgment and one which must go to full trial for resolution.[110] A prior case which had gone to full trial on the agency issue was *Seidl v. Greentree Mortgage Co*. The defendant in this case hired a single contractor on a one-time, flat fee basis to conduct an e-mail marketing campaign on its behalf. Greentree provided the body of the advertisement but left the time, manner, and choice of recipients up to the contractor, Mark Van Keuren, who used his own equipment for the job.[111] Van Keuren falsified the "from:" and "reply to:" information in his e-mail headers, electing to use the address "nobody@localhost.com." Unfortunately, the domain name localhost.com had been registered, apparently as a gag, by the plaintiff computer science student who received over 7,000 of the undeliverable advertisements as well as numerous complaints, causing his computer to crash. The plaintiff's claim failed as Greentree was able to show that Van Keuren was an independent contractor whose forgery Greentree had no knowledge of. The court also frowned on Seidl's reason for bringing the suit. The student was an anti-spam activist who wished to publicize the adverse consequences to companies who get involved with spamming. Such efforts at changing the law, the court reasoned, would be more effectively addressed in the legislative arena. Seidl's pro-activism on the socio-political issue of spamming, as Latham[112] hinted at, had done his chances at winning few favors.

The decisions in *NHCD* and *Seidl* appear to offer companies a form of legal insulation from the consequences of spamming by merely engaging an independent contractor to do the job for them. As D'Ambrosio points out,[113] this leaves ISPs with the unhappy predicament of deciding whether it is strategically viable to go after the advertising companies themselves or whether simply to attempt to stop the contract e-mailers from sending the spam. However, it is not yet clear whether the judiciary in other jurisdictions will follow the reasoning of the District Courts in Iowa and Colorado. In this regard

(N.D. Iowa 2000).

110. *Id.* at 1279–80.

111. Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292 (D. Colo. 1998).

112. Latham, *supra* note 91, at 1649.

113. D'Ambrosio, *supra* note 108, at 239.

it is certainly worth pointing out that due to the summary nature of the judgment in *NHCD* and the court's disapproval of the plaintiff's ulterior motives in *Seidl*, a future court may well distinguish such cases and re-examine the agency issue.

The preceding case law has demonstrated the fact that litigation, particularly for ISPs and relay operators,[114] has proved to be a powerful tool in the fight against spam. As well as actions for trespass to chattels, trademark infringement, breach of contract, other lesser used causes of action include nuisance,[115] unfair competition,[116] deceptive trade,[117] unjust enrichment,[118] negligence,[119] defamation,[120] fraud, and misrepresentation.[121]

In bringing suits against spammers, ISPs often use many different causes of action simultaneously. For example, in *Typhoon v. Kentech Enterprises,* the plaintiff ISP sued the defendant spammer claiming misappropriation of name and identity, trespass to chattels, unjust enrichment, and unfair competition, as well as violations of both the Lanham and Electronic Communication Privacy Acts.[122] Despite this success, members of the judiciary[123] as well as academics[124] have expressed their displeasure with the use of common law remedies to control the problem of spam. Their argument is to the effect that spam is such a unique and novel problem that it can only be effectively addressed through specifically tailored legislation. Such legislation, Kelin adds, would also manifest transparency and public accountability as well as, perhaps, giving rise

114. Relay operators have been successful in suing spammers under many of the same legal headings as ISPs have. In particular, trespass has proved to be successful. *See also* Sorkin, *supra* note 14, at 362–63.

115. Report and Recommendation, America Online, Inc. v. Christian Bros., No. 98 Civ. 8959 (DAB) (HBP) (S.D.N.Y. 1999).

116. Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q. (BNA) 2d 1020, 1023–24 (1998).

117. Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1298 (D. Colo. 1998).

118. Am. Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851, 854 (E.D. Va 1999).

119. Complaint for Plaintiff, America Online, Inc. v. Dayton, No. 98-1815-A (E.D. Va. 1998), *available at* http://legal.web.aol.com/decisions/dljunk/daytoncomp.html.

120. *Seidl*, 30 F. Supp. 2d 1292.

121. Complaint for Plaintiff, Bigfoot Partners, L.P. v. Cyber Promotions, Inc., No. 97 Civ. 7397 (S.D.N.Y. 1997), *available at* http://www.jmls.edu/cyber/cases/bf-cp0.html.

122. Complaint for Plaintiff, Typhoon, Inc. v. Kentech Enters., No. CV 97-6270 (S.D. Cal. 1997), *available at* http://legal.web.aol.com/decisions/dljunk/typhoonc.html.

123. *E.g.*, *Seidl*, 30 F. Supp. 2d at 1319 (Johnson, C.J.).

124. *See, e.g.*, Kelin, *supra* note 53, at 435–36; Moorefield, *supra* note 45, at 10 (proposing federal legislation as most promising means to address problems with unsolicited e-mail). '

to a right of recourse for individual e-mail users effected by spam.[125] Furthermore, the sheer expense of litigation, together with the uncertain status of the law in relation to junk e-mail and the pressure applied by various anti-spam lobbying groups, has led to the enactment of legislation.

C. U.S. Legislative Efforts Against Spam and Two Constitutional Barriers

Spam legislation in the U.S. has proven to be reasonably successful at the state level, but efforts to enact nationwide federal laws have proven to be abortive. Nevada became the first state to pass a statute regulating unsolicited commercial e-mail in 1997,[126] with California, Washington and Virginia following closely behind. The laws of these four states then became models for other state legislatures around the country and, at the time of writing, twenty-six states had passed laws regulating junk e-mail to a greater or lesser degree.[127] These state laws vary considerably in their approach to tackling the spam problem, but the most commonly targeted practices in the statutes are those which involve the concealment of the sender's identity. In many states, it is now unlawful to falsify the point of origin and transmission path of unsolicited e-mail advertisements. Washington state law, considered one of the most stringent, expressly forbids the use of a third party's domain name without consent; although, it may be argued that other states implicitly forbid this by making reference generally to "routing information."[128] In Washington, as well as Illinois, the use of misleading information in the subject line (spammers often use deceptive subject titles such as "Re: Your E-mail" in order to encourage users to open them) is prohibited, while Nevada law requires that e-mail advertisements should contain the true name, geographical location, and e-mail address of the sender.

Affirmative labeling requirements have proven to be popular in other states. In Tennessee, the character string 'ADV:' must begin the subject line of all commercial email solicitations, with the exception of advertisements promoting goods or services of a

125. Kelin, *supra* note 53, at 443.

126. Alan Cohen, *Can the Spam: Bills Declare War on Junk E-Mail*, N.Y.L.J., Sept. 15, 1997, at S2.

127. A list of the states is maintained at http://www.spamlaws.com/state/index.html (last visited Feb. 9, 2003).

128. Fisher, *supra* note 28, at 401–02.

sexually explicit nature where the string 'ADV: ADLT' must be used. One problem with this type of regulation, particularly at the state level, is that for it to function effectively, the same law would need to be in force in every other jurisdiction from which an e-mail user is likely to receive spam. For instance, if the federal Unsolicited Commercial Electronic Mail Choice Act of 1997[129] had ever come into force, e-mail advertisements would have had to carry the label 'advertisement' in the subject line, leaving e-marketers in Tennessee with conflicting obligations and tautologically labeled advertisements.[130] Several jurisdictions, including Louisiana and California, have given legal force to ISPs' network policies by banning the sending of spam in violation of the policy set by an ISP. In the Californian law, the spammer must have actual notice of the network provider's policy, while the Louisiana law is silent on the issue of notice. Some state laws include the mandatory provision of opt-out procedures for every unsolicited e-mail, while Delaware law goes further, requiring the pre-existence of a business relationship before the sending of any commercial e-mail, which seems more along the lines of an opt-in mechanism. As regards remedies for violations of the various state laws, statutory damages range from $10 per message received by individuals in Nevada, up to $500 in Washington, with daily caps ranging from $5,000 in Tennessee, through $25,000 in Oklahoma, to infinite liability in Washington.

The abundance of state legislation dealing with spam is due, in part, to the absence of federal legislation in this area. The lack of federal law is by no means an indication of political ignorance of the problem—to date at least fourteen federal bills have been proposed and have died either in Congress or the Senate.[131] The proposed laws have ranged from amendments to the 1991 Telephone Consumer Protection Act to include e-mail solicitations (effectively, an outright ban on spam), labeling, point of origin, and content-based restrictions such as those adopted at state level. Samoriski identifies the probable—and mainly political—reasons behind the failure of so many federal bills:

> …the likelihood of any legislation that might upset the powerful

129. Unsolicited Commercial Electronic Mail Choice Act, S. 771, 105th Cong.

130. This problem has been compounded at the state level by the recent introduction of a Pennsylvania law that requires the string "ADV- ADULT" to be used at the start of the subject line of a message promoting sexually explicit products or services. Fisher, *supra* note 28, at 402-03.

131. For an up-to-date list, *see* http://www.cauce.org/legislation/index.shtml (last visited Feb. 11, 2003).

> commercial media interests that are driving the development of the Internet is doubtful. Congress, sensitive to the media it must rely on to get re-elected, has attempted to straddle the fence between what the industry wants and what users would prefer. The result has been the appearance of legislation that may be unconstitutional, does too little, favors industry interests and/or is directed at legitimizing [unsolicited commercial e-mail] for marketing by putting 'spammers' out of business.[132]

If a federal law on spam does eventually receive the President's signature, the legislature will have to give careful consideration to what approach is taken, due to the constitutional barriers that have arisen to any statutory solutions to the spam problem.

1. First Amendment Issues

The First Amendment to the United States Constitution states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press."[133] Advertisers, pornographers and slanderers have all attempted to invoke the First Amendment to defend their actions and a large body of jurisprudence has developed accordingly. Significant for the purposes of a junk e-mail perspective is the degree of Constitutional protection offered for commercial speech in the landmark decision in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*,[134] where the Supreme Court annunciated a four-part test to determine the constitutionality of statutes:

> At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted government interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.[135]

In determining whether a statute is "not more extensive than is necessary," the court in *Board of Trustees of State University of New*

132. Samoriski, *supra* note 79, at 685.

133. U.S. CONST. amend. I.

134. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557 (1980).

135. *Id.* at 566.

York v. Fox[136] held that the regulation did not have to be the least restrictive means available, but that the First Amendment merely requires a reasonable fit between the goal and the means, i.e., that there be a measure of proportionality. However, in *City of Cincinnati v. Discovery Network, Inc*. it was found that existence of other less restrictive alternatives would be a factor in determining whether the "fit" between ends and means is reasonable.[137]

The earliest litigant to raise the First Amendment protections in the course of spam proceedings was the plaintiff in *Cyber Promotions, Inc. v. America Online, Inc*.[138] There, the highly litigious Cyber Promotions filed an action against AOL claiming that AOL's obstruction and filtering of the plaintiff's spam was in violation of its right to free speech. In rejecting this contention, the U.S. District Court for the Eastern District of Pennsylvania held that an ISP is neither a state actor nor a manifestation of the state and thus, its actions are not subject to First Amendment review.[139] An important factor in this regard is that an ISP does not exercise any municipal powers that are traditionally the prerogative of the state. This finding was upheld by the court in *CompuServe v. Cyber Promotions*, a case discussed in detail above, where Cyber again raised the First Amendment argument, this time in defense of its activities.[140]

Legislation and First Amendment scrutiny thereof is a different matter. To pass constitutional muster, a statute that restricts legal and non-misleading commercial speech must, under *Central Hudson*, directly advance a substantial governmental interest and do so with proportionality. The first thing to note is that laws which restrict the sending of misleading or illegal spam will not undergo First Amendment scrutiny. This would, in theory, apply to laws curtailing e-mail advertisements promoting the sale of, for example, explosives or narcotics, as well as to laws which prohibit the falsification of e-mail headers and routing information, although there has been some debate on this latter point.[141] Displaying a substantial government interest seems relatively straightforward,[142] given the size of the spam problem today, its disruptive nature, and its high cost to business. As

136. Bd. of Trs. of State Univ. of New York v. Fox, 492 U.S. 469 (1989).

137. City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993).

138. Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996).

139. *Id.* at 441–44.

140. *CompuServe*, 962 F. Supp. at 1025–26.

141. *See, e.g.*, Samoriski, *supra* note 79, at 679–82 (contending that any law which goes further than requiring subject line labelling will run into First Amendment problems).

142. *See generally,* Carroll, *supra* note 69, at 272–74, 277–78.

Fisher puts it, "[t]he governmental interest in preserving the viability of e-mail as a medium of communication is likely to be considered substantial if there is a real danger that this medium will be rendered useless without regulation."[143] Similarly, under the direct advancement heading no serious legal obstacles are raised. Any of the legal approaches outlined above, be they labeling, content restrictions, opt-out schemes, or forgery prohibitions, would directly advance the governmental interests involved, leaving only the issue of proportionality. Labeling requirements, as they would protect spammers' rights to deliver mail to willing consumers without imposing any real costs or burdens, are universally accepted as being sufficiently narrowly tailored to advance the governmental interest without being more extensive than is necessary. The same might be said of opt-out registers, as an advertiser has no right to solicit consumers whom he knows are not interested, and requirements not to falsify source and routing information, given that such falsification requires greater effort than the truth. The availability of such attractive alternatives may prevent a court from upholding a statutory ban on junk e-mail. Given the large-scale cost-shifting involved in spam and its few redeeming features, a wholesale prohibition does not seem overly authoritative but, in any First Amendment inquiry, a court may view the existence of less restrictive alternatives as being a decisive factor and strike down the statute. It remains to be seen whether such a constitutional analysis takes place at the state level (an examination of the restrictive state laws of Washington and Delaware would prove interesting) or if any future federal laws come into force.

2. The U.S. Constitution Dormant Commerce Clause

The U.S. Supreme Court, in *General Motors Corp. v. Tracy*,[144] has held that the Commerce Clause[145] of the U.S. Constitution contains a negative implication, the dormant Commerce Clause, which prohibits the state regulation of interstate commerce. Although the law is not absolute, states cannot interfere with the power of the federal government to regulate interstate commerce by passing their own laws. The clause has, over time, been subject to various interpretations but the modern form prohibits state legislatures from discriminating against or unduly burdening interstate commerce. In

143. Fisher, *supra* note 28, at 409.

144. Gen. Motors Corp. v. Tracy, 519 U.S. 278, 287 (1997).

145. The Commerce Clause states that Congress shall have Power . . . to regulate Commerce . . . among the several States. U.S. CONST. art. I, § 8, cl. 3.

American Libraries Association v. Pataki, a federal court held that the Internet, due to its effective similarity to other traditional instruments of interstate commerce such as the highway, railroad, or postal service, falls within the scope of the Commerce Clause.[146] In *Edgar v. MITE Corp*., the Supreme Court outlined the 'extraterritoriality doctrine.'[147] This means that the Commerce Clause precludes the application of a state statute to commerce that takes place wholly outside of the state's borders, whether or not the commerce has effects within the state. Furthermore, according to the decision in *Pike v. Bruce Church, Inc*., even if a state law regulates evenhandedly and does not directly discriminate, it can still violate the Clause if it imposes a burden of interstate commerce which is clearly excessive in relation to the putative local benefits.[148] Given these stringent restrictions, it is hardly surprising that two state laws regulating spam have fallen afoul of the dormant Commerce Clause.

The state laws in question were those of Washington and California and they were found to be unconstitutional respectively, in *State of Washington v. Heckel*[149] and *Ferguson v. Friendfinders, Inc*.[150] In both instances, the lower courts offered no analysis and neither opinion revealed the court's reasoning—the orders were brief and to the effect that the respective laws were unduly restrictive and burdensome of interstate commerce. Following the decisions in *Heckel* and *Ferguson*, it became apparent that any state regulation of spam could be struck down, and the fact that federal legislation was urgently required to fill the void was pointed out by many commentators.[151] However, both cases have recently been successfully appealed, restoring the law to its former state. The Washington Supreme Court, in *State v. Heckel*,[152] in upholding the constitutional validity of Washington's Commercial Electronic Mail Act found that:

> The Act limits the harm that deceptive commercial e-mail causes Washington businesses and citizens. The Act prohibits e-mail

146. Am. Libraries Ass'n v. Pataki , 969 F. Supp. 160 (S.D.N.Y. 1997).

147. Edgar v. MITE Corp., 457 U.S. 624, 641–42 (1982).

148. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

149. State of Washington v. Heckel , No. 98-2-25480-7 SEA (Wash. Sup. Ct. 2000) (order on civil motion granting defendant's summary judgment).

150. Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 155 Cal. Rptr. 2d 258 (2002) (order sustaining defendant's demurrer without leave to amend) *available at* ttp://www.spamlaws.com/cases/ferguson.html.

151. Kelin, *supra* note 53, at 435.

152. State v. Heckel, 24 P.3d 404 (2001).

> solicitors from using misleading information in the subject line or transmission path of any commercial e-mail message sent to Washington residents or from a computer located in Washington. We find that the local benefits of the Act outweigh any conceivable burdens the Act places on those sending commercial e-mail messages.[153]

This reasoning was followed by the Californian appellate court in *Ferguson v. Friendfinders, Inc*. as recently as January of 2002, a decision which reinstated section 17538.4 of the California Business and Professions Code as good law.[154]

In one way, it seems to be a shame that the courts in *Heckel* and *Ferguson* found the state laws to be constitutional, as the decisions have removed the urgent need for a federal law on spam. Instead, the onus will now be shifted back on to state legislatures to act in the absence of a nationwide law and the uncertain legal status of spam in the U.S. will be maintained. Some U.S. commentators, such as R. Geissler, have argued that there is no need for a separate, general anti-spam law as private civil actions, self-regulatory mechanisms and 'the marketplace of ideas'[155] are adequate responses already in existence[156] The author would criticize this approach on two grounds. First, the current growth of spam and its persistent proliferation is evidence enough of the failure of currently available legal remedies to the problem. As well as this, Geissler's argument could be criticized for perpetuating the piecemeal approach to finding a solution to the junk mail problem that has thus far been applied in the U.S.. What is needed is a broad and structured legislative framework, comprising effective federal legislation as well as the continued, but limited, use of common law private civil actions.

IV. EUROPEAN LEGAL APPROACHES TO UNSOLICITED COMMERCIAL E-MAIL

A. Legislative Regulation: The European Directives

The legal approach adopted in Europe to deal with the issue of spam has been primarily one of legislating at an EU level. This is in contrast to the stance adopted in the U.S., where the law is heavily

153. *Id.* at 413.

154. *Ferguson*, 94 Cal. App. 4th 1255.

155. R. Jonas Geissler, *Whether Anti-Spam Laws Violate the First Amendment*, J. ONLINE L., art. 8 (2001).

156. *Id.* at ¶ 37.

reliant on private civil actions and industry self-regulatory measures, and is thus in line with the general approaches taken in both jurisdictions in dealing with the "evolving legal landscape" that is developing alongside the new information technologies.[157] This may be due to societal or sociological reasons, but it is more likely due, in part at least, to an absence of technical knowledge on the part of European decision-makers with regard to emerging technologies of which one hears frequent, if anecdotal, reference to. Whatever the reason, the European debate on spam has been, if not an uninformed, certainly a limited one, and the resulting proposals for legislation have been focused almost primarily on the issue of whether to adopt an EU-wide 'opt-out' or 'opt-in' scheme. The former requires the establishment or existence of a central opt-out register which would be consulted by e-marketers on a regular basis, while the latter system would involve the prohibition of unsolicited e-mail advertising without the prior consent of the consumer addressed. Although an opt-in scheme would seem to accord with the traditional values of privacy that are associated with many European countries, many parties believe that such a system may leave EU member states out in the cold as regards the development of the e-commerce sector and the Information Society as a whole. For example, this is what the Parliamentary Committee on Citizens' Freedoms and Rights, Justice and Home Affairs had to say regarding the inclusion of an opt-in scheme in the proposed Electronic Communications Data Protection Directive:

> The opt-out system will promote e-commerce in Europe, one of the major objectives of the eEurope initiative. The opt-in system will be a barrier to the same and will help encourage direct marketing companies to set up their business outside the European Union, where the legislative framework allows the opt-out for direct marketing purposes.[158]

The European Economic and Social Committee[159] and the Committee on Legal Affairs and the Internal Market[160] made similar

157. *See* Valentine, *supra* note 42.

158. Proposal for a European Parliament and Council Directive Concerning the Processing of Personal Data and and the Protection of Privacy in the Electronic Communications Sector, EUR. PAR. DOC. (COM (2000) 385 final-2000/0189 (COD)) 31 (2000).

159. Jan. 24, 2001 opinion at http://www.esc.eu.int (last visited Feb. 14, 2003).

160. Committee on Legal Affairs and Internal Market Draft Opinion on the Proposal for a Council Directive on Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, EUR. PARL. DOC. (COM 2000) 385-C5-0439-2000/0189(COD) 10

remarks in their submissions on the same debate. However, it appears that the Commission has adopted quite a different stance.

One of the limitations of a legislative solution to spam is, as Sorkin notes, the legitimization of it.[161] If a partial solution to spam is effected i.e. regulation without prohibition, the stigma previously attached to the medium will begin to erode. The result, depending of course on what type of regulation is put in place, will be an increased use of "direct e-mail marketing" by mainstream companies and a likely increase in the net costs to individual e-mail users. A 2001 Commission report on unsolicited commercial communications and data protection makes reference to the distinction between the rude and aggressive form of e-mail marketing that has become known as spam, and the potentially legitimate opt-in strategy, known as permission marketing.[162] It appears to this author that the current strategy of the Commission as regards unsolicited commercial e-mail is to remove the "spammers" from the equation, leaving room for permission marketing to take seed and e-commerce to grow. This point is worth bearing in mind through the following examination of the development of substantive law through several EU directives, certain provisions of which either directly or indirectly regulate the sending of unsolicited commercial e-mail.

1. The Data Protection Directive

The Data Protection Directive,[163] though it makes no reference to unsolicited commercial e-mail, may nonetheless have indirect legal repercussions regarding the practice of spamming. The UK Data Protection Act (1998), the statute that transposes the Directive into UK national law, defines "personal data" as "data which relates to a living individual who can be identified: from those data; or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller."[164] For this

(2001), *available at*
http://www.europarl.eu.int/meetdocs/committees/juri/20010529/435773en.pdf.

161. Sorkin, *supra* note 28, at 382– 83.

162. European Commission, Report on Unsolicited Commercial Communications and Data Protection 98 (2001), *available at*
http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf.

163. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31, http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf and http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf.

164. Data Protection Act, 1998, c.29, § 1.

discussion, the question arises as to whether individuals may be identified from their e-mail address and, therefore, whether the data procession provisions apply. The short answer is that, on the surface, it may depend on the particular address in question. For example, this author could easily be identified from the (fictitious) e-mail address "john.magee@qub.ac.uk," since any person viewing that address could trace the author to the Queen's University in Belfast and quickly identify him. The same applies to corporate domain names, which in fact, may be even easier to trace. However, it would seem that different considerations apply to an address like "jonner@yahoo.com," which gives no geographical location or useful information other than the fact that the data subject may call himself 'jonner' and that he maintains a Yahoo! e-mail account. Even so, it has been reported that the current Data Protection Commissioner, Elizabeth France, has given a strong indication that she regards all e-mail addresses as personal data for the purposes of the 1998 Act. The theory behind this view is that regardless of the anonymous nature of many e-mail addresses, because they are unique to individual users, an electronic record may be built up about a given person. Further consideration applies when dealing with what is termed sensitive personal data. Section 2 of the 1998 Act defines this as data relating to:

> the racial or ethnic origin of the subject; his political opinions; his religious beliefs or other beliefs of a similar nature; whether he is a member of a trade union; his physical mental health or condition; his sexual life commission or alleged commission by him of any offence of any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.[165]

Addresses along the lines of "billdoherty@workersparty.ie" or even "sarahsmyth@christianscience.org" arguably fall into this category, whereby the explicit consent of the data subject would be required before the processing of such information could take place.

As regards the requisite treatment of personal data, Article 7 of the Directive states that such data be collected fairly, for specified, explicit and legitimate purposes and processed in a fair and lawful manner in line with the stated purposes. Crucially, Article 14(6) requires that an individual should be given the opportunity to object

165. Stephen Groom & Osborne Clarke, *A Legal Voyage Round Unsolicited Commercial E-Mail*, May 4, 2000, *available at* http://www.marketinglaw.co.uk upon free subscription.

to the use of their personal data for direct marketing purposes and must be informed if their data is being disclosed to a third party direct marketer. Given these provisions, it could be argued that spamming in its current form i.e. involving the use of "harvesting" software to collect e-mail addresses from public Web sites and indiscriminately e-mailing those addresses and/or sell the mailing lists to third parties is forbidden by the Data Protection Directive. However, practical considerations of enforcement dictate that the Directive does not outlaw spamming, but instead should be viewed as a requirement for a degree of openness about the processing of e-mail addresses[166] and, as such, an important first move toward the fair and legitimate form of permission marketing that is envisaged for the future.

2. The Distance Selling Directive

Article 10 of this directive[167] was the first EU law provision that came close to directly regulating spam, but without actually specifically mentioning it. Article 10(1) requires the prior consent of the consumer in the case of unsolicited commercial contact by fax or automated calling machine. Article 10(2) goes on to state that other means of distance communication which allow for individual communication may only be used where there is no clear objection from the user. This article has been interpreted as meaning that an opt-in scheme (prior consent of the consumer) is required for fax and automated calls while an opt-out mechanism (no clear objection from the consumer) will suffice for other communication channels.[168] It is interesting that e-mail was not mentioned under either heading as it did exist at the time of the adoption of the Directive, just as spam was becoming a serious problem. Lloyd believes the omission is simply due to the fact that the Directive was first drafted back in 1992,[169] while Schaub opines that it may have been so drafted to keep the provision technology neutral.[170] Another possibility is that the legislature was unable at that point in time to reach a consensus on the

166. Schaub, *supra* note 11, at 101.

167. Directive 97/7/EC on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L144) 19,

http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf.

168. For an Interpretation of the Consumer Protection (Distance Selling) Regulations 2000 (SI 2000 No. 2334) which implement the 1997 EU Directive, *see* Aron Youngerwood & Sunwinder Mann, *Extra Armoury for Consumers: The New Distance Selling Regulations*,Commentary 2000(3) J. INFORMATION, LAW & TECH. (2000), http://elj.warwick.ac.uk/jilt/00-3/youngerwood.html.

169. LLOYD, *supra* note 3, § 28.19.

170. Schaub, *supra* note 11, at 101.

issue and so left open all possibilities for another day.

The opt-out regime referred to in Article 10(2) was not fleshed out any further, giving rise to a couple of possible mechanisms. Either a consumer could respond directly to every unsolicited message or an opt-out register, such as those established by the DMA, could be created. Aside from the direct marketers themselves, few people are happy with the notion of an opt-out register, be it one general register, or a collection of a number of registers grouped according to product/service orientation. Fisher correctly points out the possibility of opt-out lists being abused by unscrupulous low-volume spammers. "The public opt-out list is a singularly dangerous alternative. It might actually do more harm than good, because it would make an enormous list of valid e-mail addresses available to the entire world."[171]

The implicit creation of an opt-out regime for unsolicited e-mail by the Distance Selling Directive, without proper consideration for the practical concerns of implementation, the author would regard as being an irresponsible attempt by the legislature to be seen to be regulating a problem but, in actual fact, side-stepping the real issues.

3. The Telecommunications Directive

Along very similar lines to Article 10 of the Distance Selling Directives, Article 12(1) of the Telecommunications Directive forbids the use of automated dialing or fax machines for the purposes of direct marketing without the prior consent of the consumer.[172] The enigmatic Article 12(2) refers to "calls made by other means of communication" and gives Member States two options as regards implementing the law for these calls.[173] Calls are not allowed: (1) without the subscriber's consent; or (2) in respect of subscribers who do not wish to receive these calls.[174] Once again, e-mail is not referred to and, in terms of interpreting Article 12(2), it would seem difficult to view the word "calls" as referring to anything other than telephone calls, presumably those made by human operators. The two regulatory options listed reveal themselves only on close inspection,

171. Fisher, *supra* note 28, at 411–12.

172. Council Directive 97/66/EC of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 24) 1, art. 12.

173. *Id.*

174. *Id.*

and refer to opt-in and opt-out regimes respectively.

However, in spite of the presence of the term "calls," four Member States (Austria, Denmark, Finland and Italy), in implementing the Directive into their respective national laws, chose to include e-mail marketing within the scope of Article 12(2) and did so in terms of an opt-in approach. The discussion regarding spam was further thrown open when the working party, installed by Article 29 of the Data Protection Directive, gave its opinion that the telecommunications legal framework should apply to e-mail communications as well as to the other listed forms of communication.[175] The fact that the other Member States interpreted the term 'calls' quite literally and thus excluded e-mail solicitation from the application of the Directive, left EU law in an unharmonized state. The Commission decided to act, drawing up a proposal for a new directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.[176] In the meantime, another Directive was reaching its final stages.

4. The E-Commerce Directive

The E-Commerce Directive became the first piece of EU legislation to explicitly refer to unsolicited commercial communication by e-mail regarding the negative consequences of spam.[177] Recital 30 states that "[t]he sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks."[178] Article 7 provides that "Member States shall lay down in their legislation that unsolicited commercial communication by electronic mail must be clearly and unequivocally identifiable as such as soon as it is received by the recipient." This provision, effectively a requirement for labeling, is an important one as it is the first legal provision emanating from the EU which attempts to tackle the spam problem head on. However, as Lloyd points out, and as has been previously indicated here, labeling requirements are only effective as part of an

175. Opinion 2/2000 of 3 February 2000 Concerning the General Review of the Telecommunications Legal Framework, document 5009/00/EN/final, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp29en.htm.

176. Commission Proposal on Protection of Privacy, *supra* note 13.

177. Council Directive 2000/31/EC of 8 June 2000 on Certain Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.

178. *Id.*

automatic filtering process if the labels used are universal. Because here they are not, the provision is only effective in helping users to nominally eliminate junk mail—by which time the damage has been done and the costs have been incurred.[179] While leaving Member States free to adopt the opt-in regime within their own national jurisdictions, Article 7(2) goes on to state that "Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by e-mail consult regularly and respect the opt-out registers in which national persons not wanting to receive such commercial communications can register themselves."[180] This provision contains a couple of problems with regard to the opt-out registers mentioned in it. The first is that they do not, in any real sense, exist—nor did they at the time of the adoption of the Directive. Perhaps the legislature envisaged that such registers would come into being upon transposition of the Directive into national law and maintained by a government body, such as the Department of Industry and Trade in the UK. The likelihood of the EU giving legislative authority to any private sector registers, such as those of the Direct Marketing Associations is unlikely given the problems associated with such schemes, as previously outlined. The other concern involving Article 7(2) is that the opt-out registers, if they were established, need only be consulted regularly, as opposed to very often or prior to the sending of an e-mail.[181] These concerns, when augmented to the problems associated with opt-out regimes generally (as discussed under the section reviewing the Distance Selling Directive), amount to a considerable argument against the opt-out approach seemingly favored by the legislature and evidenced, in this Directive, by the very formulation of the requirements.

The UK Department of Trade and Industry (DTI) considered the opt-in/opt-out argument in its second consultation paper on the implementation of the Distance Selling Directive at about the same time that the E-Commerce Directive was being finished.[182] While the DTI is clearly uncertain as to which approach to put its voice behind, the balance of the argument seemingly falls on the side of opt-in, as the draft implementing regulation in the paper made provision for an opt-in regime, with an alternative opt-out scheme appended. At this

179. LLOYD , *supra* note 3, at § 28.20.

180. Council Directive, *supra*, note 177.

181. Schaub, *supra* note 11, at 102.

182. UNITED KINGDOM DEPARTMENT OF TRADE & INDUSTRY, DISTANCE SELLING: IMPLEMENTATION OF EU DIRECTIVE 97/7/EC ON THE PROTECTION OF CONSUMERS IN RESPECT OF DISTANCE CONTRACTS - A FURTHER CONSULTATION PAPER (1999).

point in time, several other European countries, such as Germany and Sweden, were also wavering between the likely benefits and disadvantages of the two regulatory approaches on offer and, by the time the Council of Ministers sat down to discuss a proposal for a Directive on data and privacy protection in the electronic communications sector, the issue had yet to be resolved.[183]

5. The Electronic Communications Privacy Directive

The Electronic Communications Privacy Directive, first presented by the Commission in July 2000,[184] has undergone many changes since its initial proposal. The general aim of the Directive is to create rules for the use of current and future electronic communication channels that are technology neutral, ensuring that different communication methods are regulated in an equivalent manner. Despite this, the Directive begins by defining different communication methods, leaving some commentators to ask how many more such methods will need defining as advances in technology are made.[185] As if progress were trying to prove a point, a new mode of electronic communication, Short Messaging Service (SMS), which allows communication between mobile phones, came on to the scene during the adoption of the Directive. The legislature seemed to view SMS technology as falling somewhere between telephone and e-mail, and elected to include unsolicited communications by SMS within the opt-in approach. As regards unsolicited commercial e-mail, the initial proposal sought to uphold the status quo, i.e. that the individual Member States could elect between the opt-in and opt-out approaches, and this draft was accepted by the Parliament in their first reading of the proposal. However, when the Council of Ministers met again in December 2001, a massive change had occurred, whereby a compulsory opt-in approach for unsolicited commercial e-mail was put forward. The rationale for this approach is explained in Recital 40 of the new Directive:

183. Before discussion on the Electronic Communications Privacy Directive, another directive, concerning the distance marketing of consumer financial services, was adopted. Once again, e-mail was implicitly mentioned (in Art.10) but the directive simply upheld the *status quo* i.e. that Member States could elect whether to adopt an opt-in or an opt-out approach.

184. Commission Proposal on Protection of Privacy, *supra* note 13. An agreed abbreviated term for the Directive has not yet emerged and a number of terms are in use. For example, Groom & Clarke refer to it as the 'Communications Data Protection Directive,' Schaub makes reference to the 'Data Protection Directive,' while EuroCAUCE are terming it the 'E-Privacy Directive.' Schaub, *supra* note 11, at 103.

185. *See, e.g.*, Schaub, *supra* note 11, at 103.

> Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonized approach to ensure simple, Community-wide rules for businesses and users.[186]

The pan-European opt-in approach was hailed as a great victory by anti-spam activists and dealt a devastating blow to direct marketers. However, by the time the draft Directive underwent a second reading by the Parliament and was passed on May 30, 2002, two significant exceptions to the opt-in regime had been made, leaving the legal approach to spam as what has been termed a "modified opt-in" or "soft opt-in" approach.[187] The opt-in regime is created by Article 13(1) which states that "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent." ‘’‘’[188] “”The first exception is created by Article 13(2):

> Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own products or services, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.[189]

The second exception is to the effect that if the entity that

186. EC Common Position 26/2000, recital 40.

187. Groom & Clarke, *supra* note 165.

188. Second draft of 26/2000, art. 13(1).

189. *Id.* at *art*. 13(2).

receives the telephone bill for the line, on which the e-mail address is held, is other than a natural person, the modified opt-in approach does not apply. This means that if a company or partnership pays for a telephone connection, Member States retain the choice to apply an opt-out system. It should be noted that the new Directive imposes a duty on Member States to ensure that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are protected.

What is most noteworthy about the first exception created by Article 13(2) is that it allows a company to e-mail consumers whose address it obtained in the context of a *sale.* A previous draft had referred to "the context of a *purchase*." This change was effected to avoid the situation arising where marketers could argue that although no sale took place, a consumer could be included under the 'opt-out' heading as they had expressed an interest in purchasing a product. Such information could be obtained by way of a cookie, demonstrating that the individual had accessed particular parts of a Web site. Perhaps to act as a counterbalance for this measure, the original wording of Article 13(2) was altered from reading ". . . for direct marketing of its own products of services of a similar category," to simply "direct marketing of its own products or services."[190] This alteration will somewhat appease commercial Web sites that offer for a wide variety of goods and services for sale. A further amendment removed the requirement that the e-mail address needs to be obtained directly from the customer in question. This omission, though its full repercussions are unclear, would seem to indicate that a manufacturer or wholesaler who has obtained an e-mail address from the retailer who made the sale, may regard the e-mail address as being that of one of its own customers. As well as these provisions, Article 13(4) restates that the practice of disguising or concealing the identity of the sender is forbidden, and that a valid address to which a customer may request the cessation of communications must be supplied.

On the whole, the modified opt-in approach prescribed by the Electronic Communications Privacy Directive should be welcomed as a sensible regulatory solution to the problem of unsolicited commercial e-mail. By means of this approach, the EU legislative has attempted, and in this author's view has succeeded in striking an acceptable balance between the rights of individual e-mail users to be free of the cost and nuisance associated with spam, and the legitimate

190. Groom & Clarke, *supra* note 165.

interest of a commercial enterprise in using modern means of instantaneous communication to promote goods and services to its own customers and a receptive audience. The only criticism of the Directive would relate to the exception created as regards its non-applicability to e-mail received by companies and corporations. Although the legislation is obviously attempting to allow for unsolicited, business-to-business commercial communications to continue, it would be surprising if the large majority of such e-mails received in the future were not of the usual pornographic, weight loss, and get-rich-quick nature, received by ordinary office workers at their desks. In this regard, the DTI and other government bodies in the UK should seriously consider adopting an opt-in approach in relation to all unsolicited commercial e-mail, regardless of who pays the telephone bill. The Directive's provisions, assuming there are no obstacles to its adoption, should become law in all EU Member States by October 2003.

B. Non-EU Legal Approaches to Spam in the UK

Due to the existence of the substantial legal framework in place at the EU level as described above, the need for common law causes of action to deal with spam in the UK does not seem pressing, to say the least. However, given the right set of circumstances, a UK-based ISP may wish to bring a private suit on the basis of trespass for the purposes of receiving an order for damages. Such private causes of action may also arise during the time between the adoption of the Electronic Communications Directive and its implementation in UK national law.

Unsolicited commercial e-mail litigation in the UK has not proved to be fertile ground – to date, there have been no judgments recorded in UK courts on the issue.[191] The closest we have come to a written judgment was in April 1999, when VirginNet issued a writ against Adrian Paris, a businessman and president of Prophoto UK, who allegedly sent over 250,000 unsolicited e-mail advertisements from his VirginNet account.[192] According to the writ, Paris' alleged activities had generated over 1,500 complaints by VirginNet

191. Despite this, a London-based Internet company has been successful in suing a U.S. spammer. In *Bibliotech Ltd. v. Khuri*, the UK plaintiff received judgment against the defendants for spamming and was awarded damages and costs. Bibliotech Ltd. v. Khuri, CV-1344-WBH (N.D. Ga. 1999). *See* Sean Fleming, *Spam War Victory for BiblioTech*, THE REGISTER, Mar. 29, 2000, *available at* http://www.register.co.uk/content/archive/10051.html.

192. Andrew Craig, *Virgin Spammer Settles Out of Court*, VNUNET.COM, May 26, 1999, *available at* http://www.vnunet.com/News/83928.

subscribers and every effort taken by Virgin to control the problem by closing down Paris' accounts was hampered when the spammer reopened another account under an assumed name. The case subsequently settled with a reported payment of £5,000 to VirginNet and an agreement that Paris cease his spamming activities. VirginNet's solicitors were disappointed that an opportunity to set down the law on spam in the UK had been missed, but explained that the settlement offer set all the requests of the writ and so was difficult to refuse.

Had the VirginNet case gone to a full hearing, arguments alleging trespass to chattels would have been put before the court. The question arises whether the UK courts would allow for such a cause of action as has been done in the U.S.. Clerk and Lindsell on Torts have this to say, "The action of trespass has always been a remedy affording compensation for injury to a chattel in the claimant's possession. It lies for any direct and wrongful interference with possession, and is actionable *per se* (though the claimant can also recover any loss actually suffered)."[193]

Although the law on trespass in the UK does not differ dramatically from that in the U.S., a UK court considering the spam issue would likely review the area de novo. The first issue that arises is whether or not an ISP's server may be considered as goods or chattels. In *Cox v. Riley*, a case brought under the Criminal Damage Act 1971, section 10 of which defines property as "property of a tangible nature whether real or personal," this issue arose.[194] There, the appellant deliberately erased the computer programs from a printed circuit card which controlled the operation of a computerized saw. By doing so, the saw could still be used manually but its practical utility was significantly impaired, and the owner of the saw incurred the expenditure of "time and effort of a more than minimal nature."[195] The court rejected the contention that the appellant's conduct had merely affected the electronic impulses making up the program, reasoning that the conduct of Cox had caused impairment of the equipment, the restoration of which would cause the owner time and monetary expense. Not only does this decision lend support to the theory that intangible computer signals can be considered goods if part of a closed operative circuit, but also that damage can be evidenced by the significant impairment of the computer-operated

193. CLERK & LINDSELL, CLERK & LINDSELL ON TORTS § 14-02 (18th ed. 2000).

194. Cox v. Riley, 83 Cr. App. R. 54 (1986).

195. *Id.* at 56.

equipment. It would not be unreasonable for a court to hold, in the context of unsolicited bulk e-mail, that a large enough volume of spam could impair an ISP's equipment, leaving it of diminished value, though it is still functioning. As regards the question of "wrongful interference," a trespass could only be actionable if the conduct in question could be considered as being deliberate. Therefore, if an ISP has informed a spammer that they should cease their activities and the spamming persists, a cause of action for trespass could be made out.

Section 3 of the Computer Misuse Act 1990 creates an offense of unauthorized modification of the contents of any computer which was, as Chissick and Kelman note, enacted to deal with hackers and those who planted viruses, and not spammers, who did not exist in 1990.[196] However, the section 3 offense would seem to apply to spamming activities provided the requisite intent and knowledge is present. The requisite intent is:

> An intent to cause a modification of the contents of any computer and by so doing:
>
> a. to impair the operation of any computer;
>
> b. to prevent or hinder access to any program or data held in any computer; or
>
> c. to impair the operation of any such program of the reliability of any such data.[197]

In such cases where a spammer uses a false designation of origin, such could be used as an indication that the spammer knew that his conduct would cause the impairment of other computer equipment. If the CPS brought even one such case it may act as a significant deterrent to other potential junk mailers.

It has been suggested that spamming could also be construed as an offense under the 1997 Protection from Harassment Act.[198] Under the Act, it is an offense to carry on a course of conduct which amounts to harassment of another person (this is determined by an objective test), and the fact that there exists a separate offence of "putting people in fear of violence" has been cited as an indication that harassment does not require threats of violence and that a

196. MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW & PRACTICE § 2.36 (1999).

197. *Id.*

198. Groom & Clarke, supra note 164.

criminal or civil case against a "serial spammer" may prove successful.

As indicated before, such causes of action are speculative in nature due to the lack of UK case law dealing with unsolicited commercial mail and may not even be required once the new European Directive is implemented. However, this author believes that as the opt-in approach to spam is adopted around Europe and permission marketing by mainstream companies becomes the norm, e-mail users and authorities will become less and less tolerant of the seedier type of e-mail advertisement that is prevalent today and treated by many, it would seem, as no more than a minor nuisance. If this change in attitude occurs, the use of criminal sanctions, either those described above, or in the form of new, specifically tailored laws against spamming may become an issue.

V. TECHNICAL APPROACHES TO SPAM AND JURISDICTIONAL ISSUES

Although it would appear that the issues of technical solutions to spam and the perennial problems thrown up by jurisdiction and the Internet are unconnected, as the laws relating to spam in various jurisdictions become more and more disparate, international regulation of the technical measures adopted to limit spam may prove to be the only reliable method of controlling transborder unsolicited e-mail. Technical mechanisms may be regarded as a user's first line of defense against spam and have existed, as discussed earlier, since the problem of spam first arose. While anti-spam technology is in a constant state of flux, due to the continued adaptation by spammers attempting to circumvent it, the various methods used have remained the same. Spam filtering software remains the most popular, but efforts in this regard have often had the adverse effect of inadvertently blocking legitimate e-mail. This is in addition to the tremendous costs involved in constantly updating the technology as spammers become more and more familiar with it.

Other technical approaches, in particular the blocking of e-mails by ISPs with respect to information obtained from spam blacklists, encounter serious issues with regard to accountability, as has been previously mentioned. Perhaps the most effective technical solution to spam has been prevention—ensuring that spammers are unable to gain access to individual e-mail addresses. Due to the fact that most mailing lists used for the purposes of direct marketing are generated using automated harvesting software, the practice of disguising e-mail addresses by inserting a code that only humans can understand has

become common. Beke suggests that measures such as inserting the character string 'nospam' into an e-mail address or providing clues leading to a personal access code are relatively simple tasks in human terms but cannot be understood by computational linguists today.[199] The example he uses is: "[An] e-mail address is userid@host.domain.id. Take the name of the continent where I live (it has seven letters) and reverse it. Now take every other letter, starting with the first occurrence of 'c'. That's [the] personal access code."[200]

Of course, this type of measure is enormously effective but there are many instances where the provision of an e-mail address to a publicly available Web site will simply not be feasible in this format, and many users would find such evasive techniques overly cumbersome in any case.

The latest filtering technique to have emerged, and that which has resulted in the software program SpamAssassin, has involved the use of open-source software development. The instigators of the SpamAssassin project note that, unlike other spam filters, the open-source version, by utilizing the fixes of many participants has been able to take advantage of a combination of filtering techniques instead of using just one.[201] The purpose of spam filtering software such as SpamAssassin is not to eliminate the problem but merely to contain it. The rationale behind most technical approaches lies in the erection of an electronic bulwark that only the most technologically proficient spammers will be able to penetrate. As long as spam filters can eliminate the junk e-mail emanating from the average spammer, the problem will remain contained and the law can be left to deal with those who persist in sending unsolicited e-mail.

The recalcitrance of such spammers seems, at first, difficult to understand given the existence of so many technical and legal obstacles. Perhaps, for some, the prospect of a challenge and the notoriety that comes with success is the driving force but, for the rest, the motivation is entirely monetary. Spam is big business. Despite the existence in the literature of articles such as that by Fornichelli (in which is detailed the calamitous effects that an experimentation with spam had on magazine editor Erica Shames),[202] it appears that

199. Beke, *supra* note 35.

200. *Id.*

201. Andrew Leonard, *Spam vs. Spam*, SALON.COM, June 24, 2002, *available at* http://archive.salon.com/tech/col/leon/2002/06/24/spam_assassin/index.html.

202. L. Fornichelli, *When SPAM Burns YOU: Why Bulk E-Mail Can Be Bad for Business*,

unsolicited e-mail advertising can generate huge profits. The profit margins of large-scale users of bulk advertising are part of, what one might term the "dark statistics" of this issue. But in certain instances, such as litigation or liquidation, the true figures come to light. For example, Cyber Promotions, the spamming company involved in many of the important U.S. cases on unsolicited commercial e-mail, were recording sufficient operating profits to withstand many lost court battles (including one $2 million payout) before the company folded. For many smaller scale operators this is motivation enough and no legal or technical disincentive will be great enough to dissuade them. As Leonard cheekily puts it, "I have a sneaking suspicion that a gallows or a guillotine might be the only technology that really has a hope of deterring spammers."[203]

The jurisdictional problems created by the proliferation of transborder unsolicited e-mail communications represent what may prove to be an insurmountable hurdle. Despite the best efforts of many global non-governmental organizations, it seems that the differences associated with the laws of the jurisdictions of the world may prove greater than their similarities when it comes to the proposed global regulation of spam. As unsolicited commercial e-mail touches on so many aspects of the law, for example commerce, advertising, free speech, libel, intellectual property and the criminal law, it would prove to be a poor example of an activity to which to apply a global legally binding framework. Having said this, certain broad legal approaches and technical protocols could be agreed upon.

In his book, *Internet and Electronic Commerce Law in the EU*, John Dickie touches upon the jurisdictional quandary created by the Internet. In his concluding remarks on the European Community approach to electronic commerce regulation, he proposes that the traditional legal framework is an inappropriate one in which to regulate cyberspace.[204] One suggested, alternate model of governance is the "World Government Model" as outlined by the OECD.[205] This approach would involve the establishment of global rules for e-commerce under the authority of a supra national body. Although

HOMEBUSINESS J., March/April 1999.

203. Leonard, *supra* note 201.

204. JOHN DICKIE, INTERNET & ELECTRONIC COMMERCE LAW IN THE EUROPEAN UNION § 10.2 (1999).

205. OECD COMMITTEE ON CONSUMER POLICY BACKGROUND PAPER TO OECD INTERNATIONAL FORUM, GATEWAYS TO THE GLOBAL MARKET: CONSUMERS AND ELECTRONIC COMMERCE 25 (Paris, March 3–4 1997) [hereinafter Gateways to the Global Market].

some global legal frameworks have been suggested by the OECD,[206] the United Nations,[207] and the International Chamber of Commerce,[208] such instruments lack the bite of binding legal regulations, regardless of their impact upon national law.[209] Another model put forward for discussion by the OECD is that of Internet self-regulation termed the "Brave New World Model."[210] The need for this style of governance is best explained by Johnson and Post:

> Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and (1) the *power* of [the] local [government] to assert control over online behavior; (2) the *effects* of online behaviour on individuals or things; (3) the *legitimacy* of [the efforts of] a local [sovereign to enforce rules applicable to] global phenomena; and (4) the ability of physical location to give *notice* of which sets of rules apply.[211]

Although the establishment of the "Brave New World Model" would be desirable from the point of view of harmonizing current legal approaches to e-commerce issues, it has been shown in the context of unsolicited commercial e-mail that such efforts have not been successful. In this regard, it is perhaps noteworthy to point out that the groups most vocal in support of self-regulation are often proponents of direct marketing. In relation to the "World Government Model," it would appear that the development of national legal frameworks with respect to unsolicited commercial e-mail has already surpassed the point beyond which any attempt to invoke a global from of governance would be practical, or even desirable. Despite the success enjoyed by international organizations' efforts to clamp down on international criminal activities such as the trafficking of child pornography, such joint co-operative enforcement is unlikely to succeed in the field of e-commerce regulation due to the heterogeneous nature of the laws in jurisdictions across the world,

206. The OECD Privacy Guidelines in the Electronic Environment, *available at* http://www.oecd.org/subject/e_commerce.

207. U.N. COMM'N ON INT'L TRADE LAW, U.N. MODEL LAW ON ELECTRONIC COMMERCE (1996), *available at* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm.

208. Int'l Chamber of Commerce, General Usage for Internationally Digitally Ensured Commerce, *at* http://www.iccwbo.org/home/guidec/guidec.asp.

209. *See generally,* Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TULANE L. REV. 1931 (1998).

210. GATEWAYS TO THE GLOBAL MARKET, *supra* note 200, at 25.

211. David R. Johnson & David Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STANFORD L. REV. 1370 (1996) (emphasis in original).

where problems like unsolicited commercial e-mail have already been, at least, partially regulated.[212]

VI. CONCLUSION

As perhaps the most damaging and costly Internet phenomenon to both individual users and ISPs emerging in recent years, the spam problem has proved to be persistent and one which is not going away. The development of the Internet has come a long way since 1994 when Trotter Hardy was able to write that advertisements on the Web were not common due to the network's not-for-profit origins.[213] Today, the World Wide Web is, for the most part, a commercially driven information and communications tool, and it hardly comes as a surprise that many companies and individuals have taken advantage of e-mail in order to promote goods and services at almost no cost. However attractive a form of publicity this may appear to be to advertisers, unsolicited advertising by e-mail has caused massive disruption to the network particularly due to the practice of sending such e-mails by the million. Individual e-mail users end up paying a two-fold price for this. First, through the time spent in downloading, sifting through, deleting, and responding to junk e-mail and secondly, in terms of the higher access fees that ISPs are forced to charge in order to cover the costs incurred in upgrading their technology to deal with the ever increasing volume of spam. Other identifiable problems include the often-inappropriate content of spam messages, their anti-competitive nature, and the security risks posed.

The need for legal solutions to the problem became clear when, during the mid-1990s, it became apparent that the self-regulatory and vigilante methods employed to deal with spam had proved insufficient to deal with the escalating problem. In the U.S., several large ISPs litigated against known spammers and actions brought under common law trespass, as well as trademark infringement and breach of contract proved successful in cases of "aggravated spamming." These are situations where the spammer ignores requests to halt his activity, uses the domain name of a reputable company, or forges information in the header of an e-mail in order to circumvent preventative spam-filtering software. These private causes of action were augmented by the enactment of extensive U.S. state legislation

212. *See* K. A. WIMMER, COVINGTON & BURLING INFORMATION TECHNOLOGY PRACTICE GROUP REPORT, INTERNATIONAL JURISDICTION AND THE INTERNET (1999).

213. *See* I. Trotter Hardy, *The Proper Legal Regime for Cyberspace,* 55 U. PITT. L. REV. 993 (1994).

which, despite some constitutional concerns, has remained in force. To date there remains no federal legislation on the issue of spam in the U.S. with the consequent problems of a lack of uniformity and certainty in the law governing it.

By contrast, the legal approach in the EU has been almost entirely a legislative one, with little or no case law or nationally originated legislation emerging. The early EU directives which dealt obliquely with the spam issue sometimes displayed a lack of comprehension of the underlying technology but this has become less of an issue as the legislature has attempted to make the law technology neutral.

The latest and most important legislative development at the EU level has been the proposed Electronic Communications Privacy Directive with its modified or soft opt-in approach for unsolicited commercial e-mail. The directive, by providing for a Europe-wide opt-in rule with exceptions created for previous customers and subscribers who are not natural persons, marks the beginning of what has been termed permission marketing in Europe. Essentially, the Council of Telecommunications Ministers and the European Commission, with the support of Parliament, have created a regime whereby e-mail marketing will be legitimized and used by mainstream business as a marketing tool. The effectiveness of which will depend, to some degree at least, upon the extent to which "spam"—in the form it takes today—can be controlled or eliminated. In this regard, it would come as no great surprise if pressure came upon the government to introduce more severe sanctions to deal with renegade spammers. As already noted, section 3 of the UK 1990 Computer Misuse Act could be interpreted as the basis for a criminal prosecution for spamming, but it is more likely that new specifically tailored legislation would be introduced in such an eventuality.

With the European law on spam reasonably clear, focus shifts back to the U.S.—a nation which originates more spam than all the others put together—and the uncertain status of the law there. As with virtually all other laws relating to information technology in general, and to the Internet in particular, jurisdictional issues create unique problems. Transborder unsolicited e-mail cannot be dealt with effectively in terms of traditional legal systems and, as has been argued, other models of governance such as self-regulatory and supra-national approaches themselves throw up different types of problems. One possible way around these difficulties lie in the coordination of legal and technical approaches to dealing with spam. Technical measures employed in the fight against junk e-mail are usually

focused on the creation of filtering software – software which must be constantly updated as spammers become familiar with the technology and devise ingenious methods of circumventing it. Other preventative technical measures include the disguising of one's e-mail address when posting it to public Web space, so that harvesting software used to gather e-mail addresses for the purposes of spam may not understand it.

Effective coordination of legal and technical measures is easier said than done. One way in which this may be achieved is by the tailoring of technical mechanisms, such as filters, so that one would be required to break the law in order to get around them. Such a system would ensure that liability would be easier to establish but would not, on the face of it, help to control transborder junk mail. In order to achieve this, filtering software utilizing country top-level domains would need to be developed. Even this may not go far enough though as, more often than not, the top-level domain gives no indication of geographic location such as the more popular mail servers being global providers such as Yahoo! and Hotmail. Another option would be the reconfiguration of e-mail protocols, but this would be an excessively burdensome and costly one. A solution to the jurisdictional problems associated with unsolicited commercial e-mail seems elusive for the foreseeable future. In the meantime, European e-mail users and ISPs will have to be content with the European legislative framework that is in place and hope that this law will serve as a model for the future enactment of legislation in other jurisdictions.