CAN-SPAM Versus the European Union E-Privacy Directive: Does Either Provide a Solution to the Problem of Spam?

"All email users throughout the world, including consumers and businesses, struggle with the scourge of spam email."[1]

I. INTRODUCTION

Unsolicited commercial e-mail (UCE), more commonly known as spam, takes a heavy toll on business each year and has proven to be a serious international problem.[2] In 2008, spam comprised an estimated eighty percent of all e-mails sent worldwide.[3] And according to at least one source, the United

1. THE CARBON FOOTPRINT OF EMAIL SPAM REPORT (2009), http://img.en25.com/Web/McAfee/CarbonFootprint_12pg_web_REV_NA.pdf [hereinafter THE CARBON FOOTPRINT REPORT].

2. *See* PAUL BOCIJ, THE DARK SIDE OF THE INTERNET: PROTECTING YOURSELF AND YOUR FAMILY FROM ONLINE CRIMINALS 130-33 (2006) (describing cost of spam to businesses); *see also* Meyer Potashman, Note, *International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society*, 29 B.C. INT'L & COMP. L. REV. 323, 328 (2006) (describing international nature of spam problem). Businesses receiving spam, as well as internet Service Providers (ISPs), pay a heavy price because of spam. *See generally* ENISA 2009 SPAM SURVEY: WHAT ARE THE MEASURES USED BY EUROPEAN PROVIDERS TO REDUCE THE AMOUNT OF SPAM RECEIVED BY THEIR CUSTOMERS? (2009) http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/spam-survey [hereinafter ENISA EUROPEAN PROVIDERS SURVEY] (summarizing findings regarding spam's effect on European internet providers and their anti-spam mechanisms); Lisa Nuch Venbrux, *EU Agency Says Spam Fight Stabilized; Reporting, Blacklists Need Improvement*, 15 ELEC. COM. & L. REP. 141, 141 (2010) (summarizing results of survey released by European Network and Information Security Agency (ENISA)). One study found some of the larger ISPs actually have spam budgets of around one million Euros annually, and that does not even include some of their larger costs such as those incurred from customer-service calls. *See* ENISA EUROPEAN PROVIDERS SURVEY, *supra* note 2, at 22. Additionally, the ISPs surveyed responded that, on average, they tended to believe a key customer selling point is successful spam prevention. *See id.* at 24. Even businesses that were formerly more concerned with legal restrictions on their ability to market their services are beginning to realize the cost of receiving spam is more significant than the chance of restricting their ability to market their services. *See* Lisa Nuch Venbrux, *Netherlands Spam Law Expands in October to Ban Unsoliicted Messages to Businesses*, 14 ELECT. COM. & L. REP. 933 (2009) [hereinafter *Netherlands Spam Law Expands*](reporting shifting views of Dutch businesses).

3. *See e.g.* Kurt Kleiner, *Happy spamiversary! Spam reaches 30*, NEW SCIENTIST, Apr. 25, 2008, http://www.newscientist.com/article/dn13777 (describing progression and development of spamming); Symantec, *The State of Spam: A Monthly Report – November 2008*, 3 (2008) http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_11-2008.en-us.pdf (charting percentage of e-mails constituting spam through 2008); Ian Grant, *Unseen Spam Costs Growing According to Reports*, COMPUTER WEEKLY, Feb. 25, 2008 http://www.computerweekly.com/Articles/2008/02/25/229560/unseen-spam-costs-growing-according-to-report.htm (describing increases in spam traffic). In an experiment conducted by McAfee, where fifty people used the internet unprotected, researchers found people received an average of seventy UCEs per day. *See Spam Experiment Overloads Inboxes*, BBC NEWS, Jul. 1, 2008, http://news.bbc.co.uk/2/hi/technology/7482991.stm .

States generates more spam than any other country around the world.[4]

Spam often results in decreased employee productivity because of the necessity of sorting through the huge volumes of spam received every day for legitimate business e-mail.[5] Additionally, though spam filters are now common, there is always the risk that a filter will block legitimate e-mail and, for a business, missing time sensitive e-mails can be extremely detrimental to customer relations.[6] According to a study by Nucleus Research, Inc., spam costs U.S. businesses an estimated $71 billion in lost productivity, or approximately $712 per employee, per year.[7] Though these figures are difficult to verify, and different sources often suggest widely different figures, it is clear that businesses pay a high price for the convenience of e-mail communication.[8] Spamming has become so prevalent that there is now a plethora of sites devoted to calculating the cost of spam to individual businesses, as well as those offering protection from it.[9]

Spam also has a huge impact on the environment.[10] A recent study, published by McAffee, illustrates the staggering environmental costs of spam.[11]

---

4. *See* Spamhaus, *Spamhaus Statistics: The 10 Worst Spam Origin Countries*, http://www.spamhaus.org/statistics/countries.lasso (last visited July 13, 2010). According to Spamhaus, as of July 2010, the world's ten leading spam originators are, in descending order, the U.S., China, the Russian Federation, the United Kingdom, Argentina, Germany, Brazil, Romania, Canada, and Japan. *Id.*

5. *See Nucleus Research, Spam: The Repeat Offender*, 1-2 (2007), http://nucleusresearch.com/research/notes-and-reports/spam-the-repeat-offender/ [hereinafter *Nucleus Research Survey*] (reporting survey results on productivity of over 800 users). According to the April 2007 survey, average users spent an estimated one percent of their time dealing with spam each day. *Id.* at 1.

6. *See Nucleus Research Survey*, *supra* note 5, at 2 (describing problem of legitimate e-mail being blocked by spam filters); Saul Hansell, *The High, Really High Or Incredibly High Cost Of Spam*, N.Y. TIMES, Jul. 29, 2003, *available at* http://www.lexisone.com/balancing/articles/n080003d.html (describing time cost to sorting through blocked spam for legitimate e-mail). As of 2003, when spam only constituted approximately forty-five percent of worldwide e-mail sent, eBay reported problems with sellers' and buyers' e-mails being blocked by spam filters. *See* Hansell, *supra* note 6. The problem was so widespread as of then that companies began creating a position to deal with their legitimate business e-mails being blocked: I.S.P. Relations, whose job it was to remove the companies' e-mail addresses from ISP blacklists. *Id.* Since then, spam filters have become more sophisticated, but the problem has not gone away. *Nucleus Research Survey*, *supra* note 5, at 2. By 2007, Nucleus Research estimated companies using particular types of spam filters saw their employees lose, on average, over seven minutes a week looking for legitimate messages. *Id.* at 3. Nucleus Research found, in some companies, the search for lost legitimate e-mail cost $183 annually per e-mail user. *Id.*

7. *See Nucleus Research Survey*, *supra* note 5, at 1, 2 (describing its findings based on a sample of e-mail users).

8. *See* Bocij, *supra* note 2, at 132-33 (noting difficulty in determining exact cost of spam to companies).

9. *See e.g.* Spamfighter, http://www.spamfighter.com (last visited Mar. 3, 2010) (selling "Spam Filter for Outlook and Express, Windows Mail, Thunderbird and Servers"); SpamAssasin, http://spamassassin.apache.org/ (last visited Mar. 3, 2010) (offering "The Powerful #1 Open-Source Spam Filter"); Spam Titan, http://www.spamtitan.com/ (last visited Mar. 3, 2010) (advertising antispam software). One site even offers a calculator for a business's return on investment, including the annual cost of spam as a line item in the calculation. *See* Postini, Return on Investment Calculator, http://www.postini.com/services/roi_calculator.html (last visited Apr. 3, 2009).

10. *See generally* THE CARBON FOOTPRINT REPORT, *supra* note **Error! Bookmark not defined.** (detailing results of study on global environmental impact of spam e-mail).

11. *See id.* (explaining environmental cost, source, and impact of spam). According to McAfee, people analyzing the cost of spam prior to this study focused on the economic cost to businesses. *Id.* at 1. McAfee's

According to the study, spam uses thirty-three billion kilowatt-hours per year, the equivalent of the electricity used in 2.4 million U.S. homes.[12] Spam e-mailing also causes emissions of greenhouse gases at a rate equivalent to 3.1 million passenger cars using two billion gallons of gasoline.[13]

In the United States, the original responses to spam e-mail were common law actions, generally brought by internet Service Providers (ISPs), based on a variety of theories.[14] The next stage of spam control consisted of state statutory schemes.[15] Different states chose to approach the problem in different ways, and this note will examine a selected group.[16] The federal government's involvement consisted of enacting the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM Act or the Act), which preempted a majority of state legislation and restricted recourse for spamming in the US.[17]

In the European Union (EU), one of the primary concerns has been the rights of individuals to privacy, and attempts at spam regulation clearly reflect that philosophy.[18] The initial regulation of spam began with directives in which e-mail was only implicitly implicated.[19] The first attempt at express regulation was contained in Directive 2000/31/EC on certain aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), in which the European Union created an opt-out system for UCE regulation.[20] However, only two years later, the E-Commerce Directive was replaced by Directive 2002/58/EC concerning the processing of

---

focus in commissioning ICF International to conduct this study was to examine the overall impact of spam e-mail on the global environment, rather than just analyzing one country. *Id.* They described not only the volume of energy use but also its main sources. *Id.* The emissions sources include: "[h]arvesting addresses," "[c]reating spam campaigns," "[s]ending spam from zombies and mail servers," "[t]ransmitting spam from sender to receiver via the [i]nternet," "[p]rocessing of spam by incoming mail servers, "[s]toring messages," "[v]iewing and deleting spam, and "[f]iltering spam and searching for false positives." *Id.* at 3. However, the "overwhelming majority" of spam e-mail emissions come from "the process of viewing and deleting spam or searching for legitimate email [sic] erroneously trapped in spam filters (false positives)." *Id.* at 4. The study estimates spam e-mail recipients expend approximately 104 billion hours reading and deleting spam, despite the fact that spam filters block approximately eighty percent of spam. *Id.* at 7.

12. *See id.* at I (using everyday energy consumption to analogize spam energy use in key findings).

13. *See id.* (totaling emissions associated with spam). In its key findings, the study showed that though the energy use and emissions associated with spam are staggering, without spam blocking it would be considerably worse. *See id.* Indeed, spam filters and blockers save around 135 TWh of electricity per year; in other words, spam blockers have the equivalent effect of taking thirteen million cars off the road. *Id.* On November 11, 2008, an ISP took McColo Inc., then one of the largest spammers that was responsible for approximately seventy percent of spam, offline. *Id.* at 2. The resulting carbon emissions reduction was the equivalent of taking 2.2 million passenger vehicles off the road. *Id.* at 2.

14. *See infra* Part II.A.1 (explaining common law responses to spam problem).

15. *See infra* Part II.A.2 (describing state statutory solutions pre CAN-SPAM).

16. *See id.* (comparing several state statutes pre CAN-SPAM).

17. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701-7713 (2006); *see also infra* Part II.A.3 (describing enactment, requirements, effects of CAN-SPAM).

18. *See infra* note 89 and accompanying text (expounding on EU focus on rights to privacy).

19. *See infra* Part II.B.1 (describing directives regulating e-mail implicitly).

20. Council Directive 2000/31/EC, 2000 O.J. (L 178) 1 (EC) [hereinafter E-Commerce Directive].

personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive or Directive) that created the opt-in system currently in force throughout most of Europe.[21]

This Note will first describe the evolution of the Untied States' efforts to combat spam e-mail, beginning with common law solutions, and culminating with federal action.[22] Next, it will explore the development of the EU anti-spam action and member states' responses.[23] The next section will analyze the effectiveness of both the United States' and the European Union's solutions.[24] Finally, this Note will discuss potential solutions and posit that without international cooperation, the problem will never be successfully combated.[25]

II. HISTORY

A. The United States' Response to Spam

1. Common Law Responses

Before states ever took action against spam, individuals began bringing spam cases under a variety of common law theories.[26] For example, several companies successfully argued trespass to chattels cases due to the defendants' spamming.[27] Trespass to chattels occurs, *inter alia*, when one intermeddles with chattels in the possession of another.[28] However, with trespass to chattels, there are no nominal damages and liability only results where "some other and more important interest of the possessor" is affected.[29]

---

21. *See* Council Directive 2002/58/EC, 2002 O.J. (L 201) 37 [hereinafter E-Privacy Directive].

22. *See infra* Part II.A (explaining U.S. approach to spam).

23. *See infra* Part II.B (explaining EU approach to spam).

24. *See infra* Part III.A (determining successes and failures of both legislative solutions to problem of spam).

25. *See infra* Part III.B (discussing two potential private rights of action, increased ISP liability and involvement, and international cooperation).

26. *See* Amy G. Marino, Comment, *Is Spam the Rock of Sisyphus?: Whether the CAN-SPAM Act and its Global Counterparts will Delete Your E-Mail*, 32 PEPP. L. REV. 1021, 1025-29 (2005) (describing various common law responses to spam); Jeffrey L. Kosiba, Comment, *Legal Relief from Spam-Induced Internet Indigestion*, 25 U. DAYTON L. REV. 187, 194-204 (1999)(describing common law responses to spam). These legal theories included trespass to chattels, breach of contract, tortuous interference with contractual relations, and violation of trademark law. *See* Marino, *supra* note 26, at 1025-29; Kosiba, *supra* note 26, at 194. Though individuals were not barred from bringing these actions, the most successful plaintiffs were ISPs because of the hurtle of proving elements of the various actions. *See* Marino, *supra* note 26, at 1025-29, Kosiba, *supra* note 26, at 194-204.

27. *See e.g.* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015 (S.D. Ohio 1997).

28. *See* RESTATEMENT (SECOND) OF TORTS § 217 (1965) (stating elements of trespass to chattels); *see also* Kosiba, *supra* note 26, at 194-95 (explaining trespass to chattels).

29. RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965) (noting no nominal damages for trespass to chattels); *see also* Jeremiah Kelman, Note, *E-Nuisance: Unsolicited Bulk E-Mail at the Boundaries of Common Law Property Rights*, 78 S. CAL. L. REV. 363, 378 (2004) (discussing requirement for liability in trespass to chattels).

This method was most notably used by CompuServe, Inc., an ISP, in *CompuServe, Inc. v. Cyber Promotions, Incorporated*.[30] In the context of spam cases, CompuServe had no difficulty proving a possessory interest in its computer systems.[31] Nevertheless, the parties hotly contested whether the requisite harm to the chattels had occurred.[32] The court, however, concluded where there is impairment of the quality or value of a chattel as a result of another's use, the harm becomes actionable.[33] In the internet context, ISPs' impairment of quality or value can include customer dissatisfaction with the UCEs, which could lead to losing subscribers, high volume traffic causing a burden on the equipment, and storage of large volumes of undeliverable e-mail due to disguised origins.[34]

In a 2003 California case, another court made it very clear there would be no recovery unless there was threatened or actual damage to the plaintiff's computer system, no matter what type of relief was sought.[35] In the early days of spam e-mail, actual injury in the form of overloaded systems and loss of customers was not improbable.[36] But as spam becomes more prevalent and technology advances, it is less likely an ISP will suffer any actual injury from large quantities of spam.[37] Another problem with using trespass to chattels is that, although an ISP would have no problem showing the requisite possessory

30. *See CompuServe*, 962 F.Supp. at 1017 (holding Cyber Promotions's spamming a trespass to chattels); *see also* Marino, *supra* note 26, at 1025-26 (describing use of trespass to chattels in spam actions); Kosiba, *supra* note 26, at 194-95 (explaining how trespass to chattels applies in spam actions).

31. *See CompuServe*, 962 F. Supp at 1021 (stating CompuServe's possessory interest in its computer systems "undisputed").

32. *Id.* (describing defendants' proposed definition for harm in trespass to chattels).

33. *See id.* at 1021-24 (rejecting defendants' interpretation of actionable trespass to chattels). The defendants argued "that physical dispossession or substantial interference with the chattel is required" for an actionable trespass to chattel and that neither was present in this case. *Id.* at 1021. The court rejected the defendants' requested definition, explaining that even without physical dispossession there can still be actionable harm. *Id.* at 1022. "Harm to the personal property or diminution of its quality, condition, or value as a result of defendants' use" can also sustain an action for trespass to chattels. *Id.*

34. *See id.* at 1022-24 (describing harm to CompuServe). The court determined the high volume of UCEs diverted the ISP's resources from its paying customers to dealing with the unwanted e-mails, thereby lowering the value of the equipment. *Id.* at 1022. This was a clear impairment of the value of the chattel, which the court noted, is actionable. *Id.* at 1022-24.

35. *See* Intel Corp. v. Hamidi, 71 P.3d 296, 300, 303 (Cal. 2003) (holding no recovery unless threatened or actual injury). In *Hamidi*, a former employee flooded the company e-mail system on six occasions over the course of two years with e-mails criticizing Intel's employment practices. *Id.* at 301. Hamidi's e-mails did not cause physical damage, service disruption, or interruption in use of the computers. *Id.* Intel sought, and the lower court granted in summary judgment, an injunction to stop Hamidi from sending the e-mails based on a theory of trespass to chattels. *Id.* at 301-02. The Supreme Court of California held trespass to chattels does not create liability for a mass unsolicited e-mailing when there is no damage to the systems and no impairment of functionality. *Id.* at 300. Intel attempted to argue that, because it sought injunctive relief, it was exempt from the requirement of injury, but the court netherless rejected that argument. *Id.* at 303.

36. *See CompuServe*, 962 F.Supp. at 1015 (showing spam caused disruptions in server).

37. *See Intel Corp.*, 71 P.3d at 303 (showing no hitch in service despite spam). The cost of spam has decreased along with the increase in sophistication of ISPs and spam filters. *See Nucleus Research Survey*, *supra* note 5, at 2-3 (listing new anti-spam techniques).

interest in its systems, an individual plaintiff might face more difficulty.[38]

2. State Legislative Solutions Before CAN-SPAM

By December of 2003, thirty-six states had enacted anti-spam statutes.[39] The statutes varied widely in methodology as well as strictness, ranging from prohibiting falsification in UCEs, to requiring opt-out provisions in e-mails, to requiring some form of labeling in e-mail subject lines.[40]

Washington's statute is one of the statutes that merely bans sending UCEs in deceptive ways—i.e. no misleading information in the subject line or concealing the point of origin of the message.[41] An interesting feature of the Washington statute is that the spammer must either be sending the mail from a Washington location, or to an address she has reason to know is held by a Washington resident.[42]

Another group of statutes encompass those containing various labeling

38. *See* Kosiba, *supra* note 26, at 196-98 (describing difficulties in pursuing trespass to chattels actions when only individual subscribers harmed). There is a potential distinction here between e-mail users who pay for their e-mail account and those who do not. *See id.* at 197. An e-mail subscriber who pays for her account has a contract with an ISP, and this gives her a possessory interest in the account. *Id.* The time that subscriber spends filtering through her e-mail, sorting, and then deleting her unwanted spam "diminishes the quality or value" of her interest in her account. *Id.* Increasingly, people do not pay anything for their acquisition or use of an e-mail address. *Id.* Such a person has no possessory interest in her account for want of a contractural agreement with an ISP. *Id.* at 198. Therefore, a person who does not pay for the use of an e-mail account may not bring a trespass to chattels action against a sender of spam because "recovery in an action for trespass to chattels is limited only to the actual damage suffered by the owner of the possessory interest." *Id.* The e-mail user acquired the address for free and the inconvenience of sorting and deleting spam does not decrease the value of her possession. *See id.*

39. *See* Marino, *supra* note 26, at 1029; *see also* Mark Morris & Troy L. Booher, *A Case for National E-Mail Regulation: State UCE Statutes Have Infirmities*, 70 DEF. COUNS. J. 355, 364 (2003) (listing all anti-spam statutes as of April 2003).

40. *See* Morris & Booher, *supra* note 39, at 357 (detailing wide range of state spam laws).

41. WASH. REV. CODE § 19.190.020 (2007); *see also* Morris & Booher, supra note 39, at 362 (discussing unlikelihood of potential dormant commerce clause conflict with WA statute).

42. WASH. REV. CODE § 19.190.020 (1). On first impression, this standard seems very difficult to meet as it is rare a spammer would only even care where her target has residency, however the standard is satisfied if the "information is available, upon request, from the registrant of the internet domain name contained in the recipient's electronic mail address." *Id.* at § (2). The spammer does not need *actual* knowledge that she is sending to Washington residents. *See* Microsoft Corp. v. JDO Media, Inc., No. C04-0515P 2005 WL 1838609, at *2 (W.D. Wash. Aug. 1, 2005) (noting actual knowledge of recipient's location not required). There are numerous ways for a court to impute the knowledge to the spammer. *Id.* For example, the spammer knows of her recipient's Washington residence "if residency information of an email [sic] is available from the domain name registrant." *Id.* Additionally, she also has knowledge where there is,

> 1) proof that the recipient's email [sic] address was included in the Washington Email [sic] Registry co-sponsored by the Washington Attorney General and the Washington Association of Internet Service Providers ("the WAISP Registry"); and 2) proof that the spammer sent millions of emails [sic] thereby putting him on notice that a substantial volume would be received by Washington residents.

Id. The last test is very easily met, making it much more likely that a spammer will "know" her UCEs are reaching Washington residents. *See id.*

requirements for UCEs.[43] Prior to CAN-SPAM, sixteen states enacted laws with labeling requirements that generally consisted of including "ADV," "Advertisement," etc. in the subject line.[44] Utah's version required that "ADV" appear in the subject line for all UCEs, and that sexually explicit e-mail must be labeled "ADV: ADULT."[45] Direct marketers were particularly concerned about this type of legislation because such uniform labeling would make it very easy to filter the messages out using a simple spam blocker.[46]

Finally, Delaware and California enacted the most stringent of the spam legislation, though the California statute was preempted before it went into effect.[47] Both Delaware and California created opt-in schemes whereby a UCE could only lawfully be sent to a recipient who had previously consented to receive it.[48] The Delaware statute provided for criminal penalties only, whereas the California version also created a private right of action for the recipients of UCE.[49]

3. CAN-SPAM Arrives

The CAN-SPAM Act was enacted in 2003 after six years of failed attempts at congressional action.[50] Anti-spam advocates lobbied for years for the passage of a federal spam statute, but the Act finally came to fruition largely due to the efforts of lobbyists representing the interests of UCE disseminators who had formerly blocked every previous effort.[51] This change of heart coincided with the pending implementation of some of the most stringent state spam legislation to that point, notably California's.[52]

---

43. *See* Jeffrey D. Sullivan & Michael B. De Leeuw, *Spam After CAN-SPAM: How Inconsistent Thinking has Made a Hash Out of Unsolicited Commercial E-Mail Policy*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 887, 900 (2004) (explaining reasons direct marketers find labeling requirements objectionable).

44. *See id.* (describing typical labeling requirements).

45. UTAH CODE ANN. § 13-36-103 (2002), *repealed by* S.B. 92, 55th Leg., 2004 Gen. Sess. (Utah 2004); *see also* Marino, *supra* note 26, at 1030 (describing Utah statute).

46. Sullivan & De Leeuw, *supra* note 43, at 900 (explaining labeling requirement facilitates spam filtering).

47. *Id.* at 899-900 (describing CA and DE as "pioneers" in state spam legislation).

48. *Id.* at 899 (outlining opt-in system).

49. *Id.* at 899-900 (detailing CA and DE statutes).

50. *See* W. Parker Baxter, *Has Spam Been Canned? Consumers, Marketers, and the Making of the CAN-SPAM Act of 2003*, 8 N.Y.U.J. LEGIS. & PUB. POL'Y 163, 166 (2004-2005) (describing legislative history of the Act).

51. *See* Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-Mail Advertising*, 10 VA. J.L. & TECH. 5, 66 (2005) (explaining pending enactment of strict spam legislation motivating change of heart); Baxter, *supra* note 50, at 165-67 (explaining progression of congressional action or inaction on spam legislation).

52. Baxter, *supra* note 50, at 168 (remarking simultaneous Direct Marketing Association (DMA) lobbying and pending implementation of strict state statutes); *see also supra* Part II.B (describing selected state spam laws).

a. The Mechanics of the Act

Much to the chagrin of many anti-spam advocates, the CAN-SPAM Act is not a total prohibition on companies sending UCE, but rather, only a prohibition on sending these e-mails in certain circumstances.[53] A business may send commercial e-mail messages so long as they include an opt-out mechanism, whereby the consumer can opt out of receiving future mailings from the sender, and if the e-mail avoids the prohibited deceptive behaviors.[54]

The proscribed deceptive behavior seems to be aimed at ensuring transparency and preventing fraud in mailings of commercial electronic mail messages, rather than eliminating commercial e-mail altogether.[55] The CAN-SPAM Act prohibits sending e-mails with "false or misleading transmission information," with "deceptive subject headings," or without a working return e-mail address.[56] There is also a set of violations that can carry additional penalties including address harvesting, dictionary attacks, "[a]utomated creation of multiple electronic mail accounts," or relaying or retransmitting of commercial e-mail through the unauthorized access of computers or networks.[57] Additionally, any commercial e-mail containing explicit sexual material must bear warning labels.[58]

53. *See* 15 U.S.C. § 7704 (2006) (proscribing transmission of messages sometimes and allowing other times with opt-out provisions); Baxter, *supra* note 50, at 172 (describing Congress's approach to defining and proscribing spam); Sullivan & De Leeuw, *supra* note 43, at 888-91 (describing prohibitions of CAN-SPAM Act).

54. 15 U.S.C. § 7704(a)(1)-(3), (5) (2006); *see also* Sullivan & De Leeuw, *supra* note 43, at 888-91 (describing CAN-SPAM provisions). Technically, the Act describes the regulated e-mails as "commercial electronic mail messages," a statutory term that will be used here as interchangeable with the term UCE. 15 U.S.C. § 7704(a)(1) (2006). An e-mail is "commercial" when its "primary purpose . . . is the commercial advertisement or promotion of a commercial product or service (including content on an internet website operated for a commercial purpose)." 15 U.S.C. § 7702(2)(A) (2006). The Federal Trade Commission (FTC) enacted a regulation that further explicates the rule by explaining that an e-mail is "commercial," within the meaning of the Act, only when it is commercial speech under the First Amendment. 16 C.F.R. § 316.3 n.1. The regulations also provide guidance for "mixed content" e-mails with a commercial and a non-commercial purpose. *See Aitken v. Communications Workers of America*, 496 F.Supp. 2d 653, 662-63 (E.D. Va. 2007) (delineating between primarily commercial e-mails and non-commercial e-mails).

55. *See* 15 U.S.C. § 7704(a), (b), (d) (2006) (listing prohibited spamming behavior); *see also* John Soma, Patrick Singer & Jeffrey Hurd, *Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions*, 45 HARV. J. ON LEGIS. 165, 166 (2008) ("The CAN-SPAM Act does not outlaw unsolicited or spam e-mail per se"); *see also* United States v. Kilbride, 507 F. Supp. 2d 1051, 1058 (2007) (finding defendants had used deceptive practices in sending spam and were thus liable).

56. 15 U.S.C. § 7704(a)(1)–(3) (2006).

57. 15 U.S.C. § 7704(b) (2006); *see also* Sullivan & De Leeuw, *supra* note 43, at 891 (explaining provision in act for "egregious spam activity"); D. Reed Freeman, Jr. & Christopher M. Loeffler, *Ninth Annual Institute on Privacy and Security Law: CAN SPAM*, 935 PLI/PAT 287, 293 (2008) (defining each aggravated violations).

58. 15 U.S.C. § 7704(d) (2006). The Act does not altogether prohibit unsolicited e-mails containing sexual material. *Id.* Rather, so long as the subject heading, or the initially viewable material, contains the notice or notices required by the Commission it is permissible under the CAN-SPAM Act. *Id.* Additionally, "sexually oriented material" is defined as "material that depicts sexually explicit conduct . . . unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters." 15 U.S.C. § 7704(b)(4) (2006). The FTC has also promulgated the Adult Labeling

Another significant aspect of the CAN-SPAM Act is its enforcement.[59] The CAN-SPAM Act provides for federal enforcement through the Federal Trade Commission (FTC), as well as some civil enforcement that can be brought by either state attorney generals or ISPs.[60] An important new development in the FTC's ability to enforce the CAN-SPAM Act is the recent enactment of the Undertaking Spam, Spyware, and Fraud with Enforcers Beyond Borders Act of 2006 (SAFE WEB Act).[61] The SAFE WEB Act extends the FTC's reach outside of U.S. borders.[62]

State roles are restricted in CAN-SPAM Act enforcement by federal action, but ISPs have relatively broad rights to bring suit.[63] States can bring actions under the CAN-SPAM Act to get injunctions and money damages on behalf of residents, but a state is limited insofar as there is pending federal action on the same matter.[64] ISPs are limited to suits where they have been adversely affected by the behavior, and the adverse effect results from UCEs that violate the CAN-SPAM Act, not UCEs permitted by it.[65] Notably lacking in the CAN-

Rule, pursuant to this section of the CAN-SPAM Act, creating further labeling requirements. *See* Freeman, *supra* note 57, at 292-93 (listing Adult Labeling Rule requirements).

59. *See* 15 U.S.C. § 7706 (providing for enforcement generally); *see also* Sullivan & De Leeuw, *supra* note 43, at 891 (describing enforcement under CAN-SPAM); Baxter, *supra* note 50, at 174-75 (discussing lack of private right of action under CAN-SPAM Act). Suits by ISPs under the CAN-SPAM Act can result in substantial awards. *See* Facebook, Inc. v. Wallace, No. C 09-798 JF (RS), 2009 WL 3617789 at *2 (N.D. Cal. Oct. 29, 2009) (resulting in statutory CAN-SPAM damages amounting to $710,737,650); Myspace, Inc. v. Wallace, No. CV 07-1929-ABC (AGR), 2008 WL 1766714 at *5 (C.D. Cal. Apr. 15, 2008) (awarding plaintiff CAN-SPAM statutory damages totaling $384,167,700).

60. 15 U.S.C. § 7706(a), (f), (g) (2006) (providing for federal, state, and ISP enforcement); *see also* Sullivan & De Leeuw, *supra* note 43, at 891 (describing CAN-SPAM enforcement).

61. Undertaking Spam, Spyware, and Fraud with Enforcers beyond Borders Act of 2006 Pub. L. 109-455, 120 Stat. 3372 (2006).

62. *See id.*; FEDERAL TRADE COMMISSION, THE U.S. SAFE WEB ACT: THE FIRST THREE YEARS, A REPORT TO CONGRESS i (2009) [hereinafter THE FTC REPORT ON SAFE WEB] (containing FTC report, due three years after SAFE WEB enactment, regarding new enforcement with Act); *see also FTC's Report to Congress Highlights U.S. SAFE WEB Act Enforcement Authority*, 14 ELECTRONIC COM. & L. REP. 1839 (2009) (describing FTC urging Congress's removal of sunset provision from SAFE WEB Act expiring 2013); *In first SAFE WEB Act Use, FTC Shares Data With Australia, Canada to Stop Spammers*, 12 ELECTRONIC COM. & L. REP. 969 (2007) (describing first FTC use of SAFE WEB Act to increase international cooperation); *House Votes to Boost Cross-Border Law Enforcement*, 11 ELECTRONIC COM. & L. REP. 1178 (2006) (reporting House passage of SAFE WEB Act); Michael Warnecke, *FTC Reports CAN-SPAM Act is Working, but Seeks Broader International Authority*, 11 ELECTRONIC COM. & L. REP. 9 (2006) (describing FTC urging for passage of SAFE WEB Act); *Senate Commerce Approves SAFE WEB Act to Bolster FTC's Ability to Cooperate Abroad*, 10 ELECTRONIC COM. & L. REP. 1212 (2005) (reporting initial Senate Committee approval for SAFE WEB Act).

63. *See infra* notes 64-65 and accompanying text (describing state and ISP action).

64. *See* 15 U.S.C. § 7706(f)(8) (2006). When a federal agency brings an action against a spammer, the state may not bring its own case until the federal action is no longer pending. *Id.*

65. *See id.* at (g)(1); *see also* Christine Mumford, *Ninth Circuit Prepares for Docket Packed with CAN-SPAM, Mobile Marketing Issues*, 13 ELEC. COM. & L. REP. 1483 (2008), (listing pending Ninth Circuit case determining what "adversely affected" entails). To have standing, the plaintiff must be both an ISP and have suffered actual adverse effects caused by the statutory violations of the defendant. *See* 15 U.S.C. § 7706(g)(1) (2006); *see also* Gordon v. Virtumundo, Inc., 575 F.3d 1040, 1049-50 (9th Cir. 2009) (describing standing for ISPs); Asis Internet Services v. Azoogle.com, Inc., Nos. 08-15979, 08-17779, 2009 WL 4841119, at *1 (9th Cir. Dec. 2, 2009) (setting forth standing components).

SPAM Act is any provision for private rights of action beyond those of ISPs.[66] Though anti-spam activists believed a private right of action was necessary, the Direct Marketing Association (DMA) lobbied vociferously against its inclusion, and one state representative even pledged to kill any bill including one.[67]

b. CAN-SPAM Act Preemption

Partly because of the proliferation of disparate state laws dealing with spam, Congress also included a preemption clause in the CAN-SPAM Act.[68] Congress found different spam laws in different states made it difficult for "law-abiding businesses" to comply because of the nature of internet interactions.[69] In these circumstances, businesses face the difficulty of knowing exactly which law to follow for each e-mail address because e-mail addresses do not specify geographic location.[70]

The Act states that "any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, *except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto*" is preempted.[71] Thus, state attempts to regulate or prohibit the type of commercial e-mailing the Act has explicitly allowed—i.e. when a company has a legitimate mailing address and employs no deceptive practices, etc.—are preempted.[72] The preemption of

66. *See* Baxter, *supra* note 50, at 174-75 (explaining no private right of action in CAN-SPAM Act).

67. *See id.* (describing opposition to CAN-SPAM private right of action); *see also supra* note 38 (describing difficulty facing private plaintiffs using traditional common law methods of litigation).

68. *See* 15 U.S.C. § 7701(a)(11) (2006) (stating congressional finding); 15 U.S.C. § 7707(b) (2006) (enacting state law preemption); *see also* Katherine Wong, *The Future of Spam Litigation After* Omega World Travel v. Mummagraphics, 20 HARV. J.L. & TECH. 459, 463 (2007) (discussing Congress's intent to homogenize spam law).

69. *See* 15 U.S.C. § 7701(a)(11) (2004) (mentioning impact of different regulation on businesses).

70. *See id.*

71. 15 U.S.C. § 7707(b) (2006) (emphasis added).

72. *See* 15 U.S.C. § 7707(b)(1) (stating Act supersedes state law); *see also* Wong, *supra* note 68, at 462-63 (explaining CAN-SPAM Act preemption). Many defendants have litigated whether various plantiffs' state law claims were preempted by CAN-SPAM. *See* Asis Internet Servs. v. Visaprint USA, Inc., 617 F. Supp. 2d 989, 992-93 (N.D. Ca. 2009) (following preemption analysis from *Consumerbargaingiveaways*); Asis Internet Servs. v. Consumerbargaingiveaways, LLC, 622 F. Supp. 2d 935, 944 (N.D. Ca. 2009) (rejecting preemption challenge to CA staute as defendants interpreted exemption to exception too narrowly); Ferron v. Subscriberbase Holdings, Inc., No. 2:08-cv-760 2009 WL 650731, at *5 (S.D. Ohio Mar. 11, 2009) (finding CAN-SPAM Act did not preempt Ohio laws); Burgess v. Eforce Media, Inc., No. 1:07cv231 2007 WL 3355369, at *7 (W.D.N.C. Nov. 9, 2007) (holding CAN-SPAM does not preempt state common law rights of action); Facebook, Inc. v. ConnectU, LLC, 489 F. Supp. 2d 1087, 1094 (N.D. Ca. 2007) (holding CA statutes preempted because neither "purport to regulate false or deceptive email [sic]"); Free Speech Coalition, Inc. v. Shurtleff, No. 2:05cv949DAK 2007 WL 922247, at *9 (D. Utah Mar. 23, 2007) (holding Utah statute falls under preemption exception for computer crimes); Beyond Systems, Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 538 (D. Md. 2006) (rejecting preemption argument for Maryland statute because statute not "*inconsistent with CAN-SPAM*") (emphasis in original).

state law, except when a state is proscribing misleading or deceptive spamming, seems a clear continuation of the congressional intent to legalize some types of UCEs while prohibiting others.[73] However, this preemption applies only to state law specifically created to deal with spam, so CAN-SPAM does not preempt state common law responses to electronic mail through established law such as tort and contract law.[74]

It is not entirely clear, however, exactly what is left within the state's jurisdiction to specifically legislate on spam.[75] Certainly, the Act seems to have preempted most state lawmaking, but states have nevertheless continued attempts to legislate in this area.[76] One important case in determining the extent of remaining state legislative jurisdiction is *Omega World Travel, Inc. v. Mummagraphics, Incorporated*.[77] At the time, Oklahoma state law essentially created strict liability for immaterial errors in UCEs.[78] The statute seemed to

73. *See* 15 U.S.C. § 7701(b) (2006) (stating Congress's determination on UCEs). In its determination, Congress describes the right of recipients to decline further receipt of UCEs but not to prevent them entirely. *See* 15 U.S.C. § 7707(b)(3) (2006); *see also* Soma, *supra* note 55, at 166 (explaining Act allows some UCEs and not others).

74. 15 U.S.C. § 7707(b)(2) (2006) (exempting state law not specific to spam from preemption). The statute specifically includes that "[s]tate trespass, contract, or tort law" are not specific to UCEs. 15 U.S.C. § 7707(b)(2)(A) (2006).

75. *See infra* notes 80-84 and accompanying text (explaining difficulty determining states' remaining role). Another issue affecting states' roles in spam regulation is the Dormant Commerce Clause. *See* Taiwo A. Oriola, *Regulating Unsolicited Commecial Electronic Mail in the United States and the European Union: Challenges and Prospects*, 7 TUL. J. TECH. & INTELL. PROP. 113, 134-40 (2005) (describing Dormant Commerce Clause issues surrounding state action on spam).

76. *See* Jeffrey D. Neuburger, *New Media, Technology and the Law: A Summary of Key Legal Developments Affecting Technology and Emerging Business Models*, 961 PLI/PAT 147, 217-18 (2009) (describing several state attempts to legislate after CAN-SPAM). There is still a significant role for states in spam litigation even if it seems as if most of their efforts have been preempted. *See* Microsoft Corp. v. JDO Media, Inc., No. C04-0151P 2005 WL 1838609, at *3 (W.D. Wash. Aug. 1, 2005) (awarding plaintiff $24,125,000 under Washington's Commercial Electronic Mail Act (CEMA)). In *JDO Media*, though Microsoft pled both a CAN-SPAM as well as a state law claim, the state law claim proved far more valuable. *See id.* The statutory damages for each e-mail was $1000, and because spam e-mail is sent in such high volume, astronomical awards can result. *Id.* Indeed, the defendant in this case sent 24,125 e-mails in violation of the Washington statute to accounts maintained by the plaintiff. *Id.*

77. 469 F.3d 348, 354-55 (4th Cir. 2006) (determining appropriate definition of "falsity" and "deception" in CAN-SPAM preemption exception); *see also* Jay Reyero, *The CAN-SPAM Act of 2003: A False Hope*, 11 SMU SCI. & TECH. L. REV. 195, 218-23 (2003) (discussing *Omega World Travel* and its effect on preemption). In *Omega World Travel*, Mummagraphics, Inc. brought an action under the CAN-SPAM Act and Oklahoma state law due to inaccuracies in e-mails sent by Omega World Travel, Inc. and its wholly owned subsidiary. *See* 469 F.3d at 350-51. The district court granted summary judgment to Omega holding the CAN-SPAM Act preempted the OK statute and that, because the errors were immaterial, Mummagraphics had no actionable claims under the Act. *Id.* at 352. Mummagraphics appealed stating that the CAN-SPAM Act did not preempt OK law because the statute fell within the Act's exception for state laws prohibiting "falsity or deception." *Id.* at 352-53.

78. OKLA. STAT. ANN. tit. 15, § 776.1A (West 2005) amended by OKLA. STAT. ANN. tit. 15, § 776.A (2008) (; *see also Omega World Travel*, 469 F.3d at 353 (considering language of OK statute). The statute provided that a sender of commercial e-mail is liable in the event that he or she "knows or has reason to know" that the e-mail, "[c]ontains false . . . information which purposely or negligently injures a person." *Omega World Travel*, 469 F.3d at 353.

directly oppose the intent of the CAN-SPAM drafters.[79] The court determined the exception to CAN-SPAM preemption is not so broad as to allow a state to legislate on immaterial errors because that would create, "a loophole so broad that it would virtually swallow the preemption clause itself."[80]

The Act also allows internet access service providers, the same as ISPs, to adopt, implement, or enforce policies regulating UCEs on their servers.[81] Thus, when a state cannot lawfully ban the type of UCE the Act legalized, an ISP can still create a policy blocking those messages.[82] The first case dealing with preemption under the then new CAN-SPAM Act, *White Buffalo Ventures, LLC v. University of Texas at Austin*, raised a wrinkle in state preemption.[83] White Buffalo Ventures sued the University of Texas at Austin (UT) for access to its students' e-mail, based on a theory of CAN-SPAM Act preemption of UT's anti-spam policy.[84] The court, however, determined UT was not only a state actor, but also an ISP, and as such fell within the § 7707(c) exception for ISPs.[85]

B. The European Union Response to Spam

Before 1998, the only European Union action taken on spam e-mailing was found implicitly in the language of several directives.[86] It was not until the Electronic Commerce Directive, which has since been replaced by the E-Privacy Directive, that the European Parliament chose to take explicit action on the spam problem.[87]

1. Before Explicit European Union Action

In 1995, the European Union enacted 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 (Data Protection Directive).[88] The Data Protection

79. See 15 U.S.C. § 7701(b)(2) (2006) (stating primary intent to prevent only misleading UCEs); *see also Omega World Travel*, 469 F.3d at 355 (discussing Congressional intent behind CAN-SPAM Act).

80. *Omega World Travel*, 469 F.3d at 355.

81. *See* 15 U.S.C. § 7707(c) (2006). The ISP is free to enact "a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages." *Id.*

82. *See id.*

83. 420 F.3d 366 (5th Cir. 2005) (involving direct marketer challenge to University of Texas at Austin e-mail filtering system).

84. *Id.* at 370-72 (describing White Buffalo Ventures's preemption claim). White Buffalo Ventures attempted to send out mass UCEs to UT students, which UT blocked pursuant to its internal anti-solicitation policy. *Id.* at 368. White Buffalo sued UT based on the theory, among other things, that the CAN-SPAM Act preempts all state spam laws, including those from subdivisions of a state or a state actor, and thus its policy was preempted. *Id.* at 371. Were that the case, White Buffalo could not be blocked from e-mailing the students because it complied with all CAN-SPAM requirements. *See id.*

85. *See id.* at 373 (describing university's designation).

86. *See infra* notes 88-96 and accompanying text (describing European Union level action prior to 1998).

87. *See infra* notes 97-124 (describing initial anti-spam directive and current version).

88. *See generally* Council Directive 95/46/EC, 1995 O.J. (L281) 31 (EC) [hereinafter Data Protection

Directive does not specifically address the issue of spam, but rather seeks to protect people's right to privacy with respect to the processing of their personal data.[89] This directive only takes effect on spam e-mailing if e-mail addresses are considered "personal data" and if spam e-mailing involves "processing" it.[90] Although the Data Protection Directive was not specifically written to control spam, it does establish privacy as an important right in Europe, and accordingly creates high standards for the processing of private data.[91] This directive is still in force, and continues to be an important source of privacy law.[92]

The next European Union directive to indirectly touch on spam e-mailing was Directive 97/7/EC on the protection of consumers in respect of distance contracts (Distance Selling Directive).[93] Pursuant to the Distance Selling Directive, anyone acting in a commercial or professional capacity—a

Directive] (containing Commission's first attempt at European spam legislation establishing opt-out system).

89. *See id.* at art. 1 (asserting goal of Data Protection Directive). The EU legislators intended the scope of this directive to be very broad. *See* Lillian V. Blageff, *Records Retention Requirements Under the European Union Data Privacy Directive*, 17 WINTER INT'L HR J. 4 (2008) (discussing scope of Data Protection Directive). This is because a person's right to privacy in the transmission of her personal data is considered an important right that needs to be regularized among the member states. *See* Data Protection Directive, ¶¶ 7, 10, 1995 O.J. (L281) 31 (EC); *id.* at art. 1. But the European Parliament (EP) noted different standards and levels of protection afforded in different member states could have negative effects on commerce by creating distortions in competition. *See id.* at ¶ 7. Even as of 2007, the various member states have interpreted their versions of the directive in such a way that there remains uncertainty in what constitutes personal data protected under the legislation. *See* Patrick Van Eecke & Maarten Truyens, *Recent Events in EU Internet Law*, 11 No. 6 J. INTERNET L. 29, 29 (2007) (explaining recent decision determining whether IP addresses constituted personal data).

90. *See* Data Protection Directive, art. 2(b), 1995 O.J. (L281) 31 (EC). It seems evident spamming would fall within the definition of "processing of personal data" because the comprehensive list of activities is so broad as to be almost impossible to avoid. *See id.* Among other things, the mere "use" of personal data is within the scope of the term "processing," and it can be done by any means—i.e. "whether or not by automatic means." *Id.* Additionally, the definition of "personal data" is fairly broad, simply requiring it be "related to an identified or identifiable natural person." *Id.* at art. 2(a). However, as the directive is only a guideline for national laws, the language of a particular member state's law might vary enough for a different outcome. *See* John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 364-65 (2003) (discussing whether e-mail addresses are personal data pursuant to United Kingdom law).

91. *See* Data Protection Directive, art. 6, 7, 1995 O.J. (L281) 31 (EC) (expressing EU perspective on privacy). The standards for when and how data can be processed are stringent. *See id.* Without unambiguous consent, there is only a limited number of reasons data can be processed legitimately. *See id.* at art. 7.

92. *See* Ruth Hill Bro, *Government Enforcement and the Risks of Privacy Noncompliance*, 902 PLI/PAT 235, 269-70 (2007) (explaining Data Protection Directive's important role in privacy law); *see also* Case C-275/06, Promusicae v. Telefónica, 2008 O.J. (C64) 9 (enforcing Data Protection Directive); Fanny Coudert & Evi Werkers, *In the Aftermath of the* Promusicae *Case: How to Strike the Balance?*, 18 INT'L J.L. & INFO. TECH. 50, 63-65 (2010) (explaining application of Data Protection Directive to *Promusicae v. Telefónica*). Not only have the EU member states enacted privacy laws pursuant to the Data Protection Directive, but the Data Protection Directive has also influenced countries outside of the EU—Japan and Canada for example—in formation of their privacy laws as well. *See* Bro, *supra* note 92, at 269.

93. *See generally* Council Directive 97/7/EC, 1997 O.J. (L144) 19 (EC) [hereinafter Distance Selling Directive] (containing act indirectly touching on spam e-mail regulation); *see also* Magee, *supra* note 90, at 366-67 (describing connection between Distance Selling Directive and spam e-mailing).

"supplier"—must receive prior consent of another before contacting him or her through either automated calling systems or through fax.[94] However, if the supplier chooses to use other means of distance communication, presumably including e-mail, then she need only stop if she receives explicit objection from the consumer.[95] This essentially created an opt-in system for fax and automated calling, and an opt-out system for other forms of distance communication, while not specifying methods for implementation.[96]

2. The First Attempt (European Opt-Out)

In 2000, Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market went into effect.[97] In large part motivated by concern that an opt-in system would stunt developing electronic commerce, this first attempt at spam legislation allowed countries to implement an opt-out mechanism.[98] The E-Commerce Directive's first requirement, with respect to commercial e-mailing, is essentially a labeling requirement.[99] While the provision does not require specific words or symbols, e-mails must be unambiguously identified as commercial communications.[100] However, member states remain free to enact more restrictive laws.[101]

Article seven of the E-Commerce Directive creates an opt-out system with a structure that proved to be unworkable.[102] It required UCE senders to regularly check and respect registers of persons not wanting to receive these commercial

94. Distance Selling Directive, art. 2(3), 1997 O.J. (L144) 19 (EC) (defining supplier); *id.* at art. 10(1).

95. *See id.* at art. 10(2) (requiring clear objection to stop other forms of distance communications).

96. *See* Magee, *supra* note 90, at 366-67 (explaining mechanics of Distance Selling Directive).

97. *See generally* E-Commerce Directive, 2000 O.J. (L178) 1 (EC).

98. *See id.* at art. 7; NICOLA LUGARESI, EUROPEAN UNION VS. SPAM: A LEGAL RESPONSE 3 (2008) ftp://ftp.research.microsoft.com/users/joshuago/papers-2004/145.pdf (describing commercial concerns prompting initial opt-out system). Another area of concern for the drafters was that placing liability on the intermediaries, ISPs, would stunt the flow of information on the internet. *See* Patrick Van Eecke & Barbara Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 No. 4 J. INTERNET L. 3, 4 (2009). Because ISPs play the role of "mere conduits" the regime provided ways to prevent liability. *See id.* at 4-6 (describing E-Commerce Directive's limiting liability mechanisms). Thus the directive creates a set of rules providing instruction to ISPs on how to avoid liability under the regime. *See id.*

99. *See* E-Commerce Directive, art. 7(1), 2000 O.J. (L178) 1 (EC); *see* Magee, *supra* note 90, at 368 (explaining labeling requirement).

100. *See* E-Commerce Directive, art. 7(1), 2000 O.J. (L178) 1 (EC). Without a standardized labeling system, the provision proves somewhat unhelpful as a filtering mechanism. *See* Magee, *supra* note 90, at 369.

101. *See* E-Commerce Directive, art. 7(1), 2000 O.J. (L178) 1 (EC). The directive requires member states allowing unsolicited commercial communication by e-mail to have a label, however this does not restrict the member states from being more restrictive. *See id.*

102. *See* E-Commerce Directive, art. 7(2), 2000 O.J. (L178) 1 (EC) (describing creation of opt-out registers); Magee, *supra* note 90, at 369 (explaining difficulties with opt-out registers). The legislation provided for opt-out registers, where e-mail users could register their e-mail addresses, and which marketers were supposed to check from time to time. *See* Magee, *supra* note 90, at 369.

communications.[103] Opt-out registers, however, are targets for abuse because they provide spammers with lists of legitimate e-mail addresses.[104] Compliance issues also arose because the opt-out registers did not exist when the directive became effective.[105] Finally, the E-Commerce Directive created unclear duties for UCE senders by subjecting them to the vague requirement of "regularly" checking the registers.[106]

3. Current European Opt-In: The E-Privacy Directive

In 2002, the European Parliament finally managed to overcome the concerns about suppressing electronic commerce and brought the current directive regulating UCEs into force.[107] The E-Privacy Directive represents a big change in European Union policy, as it is the first legislative action explicitly taking a hard stance on UCE.[108]

a. The Mechanics of the Directive

One of the most significant aspects of the Directive is it creates an opt-in system prohibiting the use of e-mail for direct marketing purposes without prior consent from the recipient, except in limited circumstances.[109] For instance,

103. *See* E-Commerce Directive, art. 7(2), 2000 O.J. (L178) 1 (EC).

104. Magee, *supra* note 90, at 367 (disparaging opt-out registers).

105. *Id.* at 369 (noting nonexistence of opt-out registers).

106. *See* E-Commerce Directive, art. 7(2), 2000 O.J. (L178) 1 (EC); *see also* Magee, *supra* note 90, at 369 (noting registers more effective if spammers must check before sending e-mail).

107. E-Privacy Directive, 2002 O.J. (L201) 37 (EC). Not sure what to follow because it is not technically a statute); *see also* Lugaresi, *supra* note 98, at 3 (discussing tension between individuals' right to privacy and encouraging commerce). Prior to the E-Privacy Directive, the EU passed Directive 97/66/EC in 1997, which dealt with privacy in the telecommunications sector. *See* Council Directive 97/66/EC, 1997 O.J. (L 24) 1 (EC) [hereinafter Directive on Privacy in Telecommunications]; *see also* Blageff, *supra* note 89, at 3 (describing progression of Directive 97/66/EC). The EU amended the Directive on Privacy in Telecommunications in 2001 to specifically include spam. *See* Blageff, *supra* note 89, at 3 (listing amendment date and substance). The amendments, among other things, banned spam e-mail entirely unless a company was sending e-mail to a person who had made a purchase from it. *See id.* at 4. These radical changes were motivated primarily by law enforcement and intelligence agencies who were responding to the chaos of the events on September 11, 2001. *See id.* The Directive on Privacy in Telecommunications did not remain in force long, and was ultimately repealed by the E-Privacy Directive. *See id.* at 3; *see also* E-Privacy Directive, 2002 O.J. (L201) 37 (EC).

108. *Compare supra* Parts II.B.1-2 (describing action prior to E-Privacy Directive), *with infra* Part II.B.3.a (describing mechanics of current directive). The Directive mandates a minimum standard of spam regulation, but member states may choose to enact stricter laws than the Directive technically requires. *See* David Bender, *Privacy Developments—2005*, 842 PLI/PAT 9, 45-46 (2005) (describing Danish case enforcing Danish Marketing Practices Act). In a Danish case against a software company that sent UCEs from a server in Norway, the defendant attempted to argue that, because Norwegian law was less strict than Danish law, the stricter Danish law could not be enforced against it for those violations. *See id.* The court found, however, the Danish law was permissibly stricter than the general EU standard and so rejected the defendant's argument. *See id.* at 46.

109. *See* E-Privacy Directive, art. 13, 2002 O.J. (L201) 37 (EC) (limiting unsolicited communications); *see also* John Delaney, *Complying with the CAN-SPAM Act and Other Critical Business Issues: Staying Out of Trouble*, 784 PLI/PAT 123, 125-26 (2004) (explaining opt-in system in Directive); Erika Hallace Kikuchi, Note, *Spam in a Box: Amending CAN-SPAM & Aiming Toward a Global Solution*, 10 B.U. J. SCI. & TECH. L. 263,

one exception to the opt-in rule allows e-mail solicitation when the marketer obtains the e-mail address in the context of a sale of goods or services.[110] In such cases, however, only the specific natural or legal person who obtained the address may use it, and only to market that natural or legal person's "own similar products or services."[111] Moreover, companies falling within the exception are still required to include an opt-out provision.[112]

The difficulty with the exception provision is, for companies with parent or subsidiary relationships, it may be unclear exactly which natural or legal persons have the requisite relationship to qualify for the exception, and whether those persons may claim the requisite ownership of the particular products and services involved in the transaction.[113] Differences in the laws particular member states enact cause additional problems.[114] For example, the phrase "in the context of the sale" seems unambiguous, but member states are not always consistent in their interpretations of the statutory language.[115]

An additional exception to the opt-in provision lies in a member state's choice between applying the opt-in rules to natural persons only, or protecting legal persons as well.[116] The Directive does not require member states to include legal persons in the opt-in system, though it is mandatory for natural persons.[117] Considering businesses are often those hit hardest with the cost of spam, the decision seems to cut at the Directive's efficacy in the fight against spam.[118] Perhaps the disparity in European Union protection, however, is due

296-98 (2004) (describing EU opt-in system). Another important feature of the E-Privacy Directive is that there is no private right of action beyond "providers of public electronic communication networks." *See* Rick Mitchell, *EU Official Favors Broader Class Action, Breach Notice Rights in E-Privacy Proposal*, 13 ELEC. COM. & L. REP. 576 (2008) (reporting European Data Protection Supervisor's concers about lack of private right of action) (internal quotations omitted).

110. *See* E-Privacy Directive, art. 13(2), 2002 O.J. (L201) 37 (EC) (providing exception to ban on UCEs).

111. *Id.*

112. *Id.*

113. *See* Delaney, *supra* note 109, at 126 (discussing difficulty complying with Directive for large companies).

114. *Id.* at 125-26 (comparing several member states' laws enacted pursuant to Directive).

115. *Id.* at 125 (contrasting German and UK law interpreting "on-going commercial relationship"). As of 2003, the German statute seemingly required something more than a simple sale, while the UK version did not even require a sale; mere negotiations for a sale were sufficient. *See id.*

116. *See* E-Privacy Directive, art. 13(5), 2002 O.J. (L201) 37 (EC); Kikuchi, *supra* note 109, at 297 (criticizing decision leaving choice between opt-in for natural and/or legal persons to countries); *see also* Lisa Nuch Venbrux, *Dutch Telecom Reform Bans All Spam, Not Just Unwanted E-Mail to Consumers*, 14 ELEC. COMM. & L. REP. 912 (2009) (reporting recent change in Dutch law previously only banning to consumers, now including businesses recipients).

117. *See* E-Privacy Directive, art. 13(5), 2002 O.J. (L2010) 37 (EC). The Directive provides each member state with the discretion to choose how to regulate spam to legal persons. *See id.* "Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected." *Id.*

118. *See Nucleus Research Survey*, *supra* note 5, at 1. In the survey, Nucleus Research estimated that as of 2007, businesses in the United States alone were losing over seventy billion dollars a year in worker productivity. *Id.*

to the nature of the concerns the E-Privacy Directive is seeking to protect.[119]

Some member states choose not to make a distinction between legal and natural persons, though this is not consistent across all member state laws.[120] Choosing to create distinct systems for natural and legal persons could create a serious problem with compliance.[121] Indeed, due to the difficulty of determining exactly who a particular e-mail address belongs to, let alone whether it is a natural or legal person, a company attempting compliance could accidentally violate the law.[122]

Finally, like the CAN-SPAM Act, the E-Privacy Directive singles out those who send UCEs using deceptive methods.[123] This provision seems superfluous because it is unlikely that companies that fit in one of the Directive's exceptions, or who obtain prior consent, will be those employing deceptive practices, and, without an exception or consent, UCE is prohibited regardless of truthfulness.[124]

b. The 2006 Communication from the Commission

The Directive required member states to enact laws pursuant to the requirements of the Directive before October 31, 2003.[125] By the deadline, however, only a few member states enacted laws, and as a result, in March 2004 the EU ordered the delinquent states to comply.[126] Despite the threat, some member states continued to drag their feet, and in December 2004 the EU instituted proceedings against the stragglers.[127] By 2007, the member states

119. *See* E-Privacy Directive, ¶ 7, 2002 O.J. (L201) 37 (EC) (stating goals of European Union in enacting Directive). The European Parliament and Council declared that the laws enacted by various member states should seek to "protect fundamental rights and freedoms of natural persons" but with respect to legal persons, should protect their "legitimate interests." *Id.* Likely, a fundamental right would be much weightier than a "legitimate interest." *Id.*

120. *Compare* INTERNATIONAL TELECOMMUNICATION UNION, ITU SURVEY ON ANTI-SPAM LEGISLATION WORLDWIDE 47 (2005), http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf [hereinafter ITU SURVEY] (describing Portuguese anti-spam legislation applying opt-in to natural persons only), *with* ITU SURVEY at 52 (describing Swedish anti-spam legislation applying opt-in to natural and legal persons).

121. *See* Lugaresi, *supra* note 98, at 6 (hypothesizing increased simplicity in adopting opt-in for natural and legal persons).

122. *Id.*

123. E-Privacy Directive, art. 13(4), 2002 O.J. (L201) 37 (EC). The E-Privacy Directive provides that, "[i]n any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited." *Id.*

124. Lugaresi, *supra* note 98, at 6 (opining on redundancy of prohibition on deceptive UCEs).

125. *See* E-Privacy Directive, art. 17(1), 2002 O.J. (L201) 37 (EC).

126. *See* JONATHAN D. HART, INTERNET LAW, A FIELD GUIDE 565 (6th ed. 2007). By the deadline, nine member states had not yet enacted laws pursuant to the directive: France, Germany, Belgium, Finland, Greece, Luxembourg, the Netherlands, Portugal, and Sweden. *Id.* Sweden was in compliance before the EU threatened to take action and ordered non-complying member states to enact the appropriate legislation. *Id.*

127. *See id.* at 566. In response to the order, many states brought their legislation into compliance, however, due to their noncompliance, the EU instituted action against Belgium, Greece, Luxembourg, and EU newcomers Estonia and the Czech Republic. *Id.*

enacted the necessary legislation.[128]

Despite member state compliance in enacting laws as required by the Directive, the European Commission still felt it necessary to issue a communication admonishing states to improve their enforcement of spam laws.[129] In its report, the Commission declared the necessity of increased law enforcement; international cooperation, both with other member states and non EU member countries; further industry action; and development of better technology to combat spam.[130] The Commission also noted the enforcement of anti-spam laws was very inconsistent, with some agencies instituting large numbers of actions against spammers, and others bringing none.[131] Additionally, the Commission highlighted the fact that, while some forms of spam threats had been dealt with, others had been ignored.[132] In response to its findings, the Commission had a company conduct a study of member state compliance, the results of which showed member state enforcement is indeed disparate.[133]

---

128. *See id.* at 566-69 (describing member state laws as of 2007); *see also* ITU SURVEY, *supra* note 110 (listing all member states' spam laws as of 2005).

129. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Fighting Spam, Spyware, and Malicious Software*, at 11-12, COM (2006) 688 final (Nov. 15, 2006), http://eur-lex.europa.eu/LexUriServ/LexUriServ .do?uri=COM:2006:0688:FIN:EN:PDF [hereinafter *Communication on Fighting Spam*](declaring necessity of increased member state action combating spam e-mailing).

130. *Id.* at 2 (listing purposes of communication).

131. *Id.* at 6. Though the Commission was focused on member state enforcement, some members of parliament in the UK have recently begun questioning how much of a role ISPs should have in policing the internet. *See* Ali Qassim, *U.K. Parliamentary Group Launches Inquiry Into ISP Role in Catching Bad Actors on Net*, 14 ELECT. COM. & L. REP. 589 (2009) (reporting parliamentary group's objectives). Though the study is not necessarily specific to spam, a study focusing on spam might be the next step depending on the results. *See id.* (describing study objectives including determining "[w]hich entities should [pay] for the transmission of Internet [sic] traffic").

132. *See Communication on Fighting Spam*, *supra* note 129, at 6 (noting high risk threats hardly prosecuted).

133. *See* TIME.LEX, STUDY ON ACTIVITIES UNDERTAKEN TO ADDRESS THREATS THAT UNDERMINE CONFIDENCE IN THE INFORMATION SOCIETY, SUCH AS SPAM, SPYWARE AND MALICIOUS SOFTWARE 24 (Oct. 2, 2009) http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf [hereinafter MEMBER STATE ENFORCEMENT STUDY] (summarizing time.lex's findings concerning member state action against, among other things, spam); *see also* Lisa Nuch Venbrux, *European Commission Urges More Uniform Action to Fight Spam, Online Privacy Threats*, 14 ELEC. COM. & L. REP. 1485 (2009) (reporting EU Commissioner frustration with inconsistent action against spam across member states). The study reports some member states have been very active in the fight against spam through legislation and budgeting for enforcement. *See* MEMBER STATE ENFORCEMENT STUDY, *supra* note 133, at 10 (discussing anti-spam activity level of member states); *see also* Ali Quassim, *Ireland Reports Data Protection Complaints Held Steady in '07 and '08, E-Mail Spam Fell*, 14 ELEC. COM. & L. REP. 707 (2009) (describing Irish report finding spam decrease and citing enacted regulations as one cause). Other countries have been lax and, whether through lack of competence or lack of dedicated funding, have not done much to combat the spam problem. *See* MEMBER STATE ENFORCEMENT STUDY, *supra* note 133, at 10. Not surprisingly, the United Kingdom, listed as one of the worst worldwide sources of spam, is one of the underperforming member states with regard to action against spam. *See* Spamhaus, *supra* note 4 (listing UK as major spam source); MEMBER STATE ENFORCEMENT STUDY, *supra* note 133, at 90-91 (describing UK action against spam). The

III. ANALYSIS

There are clear indications that the CAN-SPAM Act has many problems: the U.S. is now the number one source of spam worldwide, and the rate at which spam dominates the overall number of e-mail communications is ever increasing, totaling approximately 120 billion messages a day. [134] Furthermore, the system in the EU, while it has seen some success, has also faced failure.[135] Although the Commission praises the Netherlands's success in cutting down on spam it is outsourcing, it is not clear it has seen much decrease in the spam it receives, considering most of the spam e-mail comes from other countries.[136]

A. Did Either the US or the EU Get it Right?

1. The Necessity of Uniformity

a. U.S. CAN-SPAM Act Preemption

Congress acted correctly when it enacted the CAN-SPAM Act, in that it created a single federally enacted law controlling UCE. Due to the nature of the internet, regulation is problematic.[137] Internet interaction disregards geographic boundaries, making the application of legal concepts that rely on these boundaries, such as personal jurisdiction, difficult to apply; nevertheless, this difficulty has not stopped courts from attempting it.[138] A person's actions on the internet may bring her under the jurisdiction of a state, without any awareness that she was interacting with citizens of that state.[139] Before CAN-SPAM, if one actually wanted to ensure compliance with every state spam law, he or she would have to comply with the strictest state law.[140] Although this

Commissioner for Information Society and Media, Viviane Reding, said that the EU as a whole must do more to combat spam. *See* Venbrux, *supra* note 133.

134. *See* Spamhaus, *supra* note 4 (declaring US worst spam offender worldwide); *see also Nucleus Research Survey*, *supra* note 5, at 1 (estimating loss of over seventy billion dollars in worker productivity in U.S. due to spam); Kleiner, *supra* note 3 (estimating spam accounts for approximately eighty percent of e-mails sent worldwide).

135. *Compare Communication on Fighting Spam*, supra note 129, at 3 (reporting Netherlands' success reducing eighty-five percent of Dutch spam), *with* Spamhaus, *supra* note 4 (listing U.K. and Germany as fourth and ninth worst spam producers, respectively).

136. *See Communication on Fighting Spam*, *supra* note 129, at 3; *see also* Oriola, *supra* note 75, at 123 (stating EU knows majority of spam originates outside of Europe); Spamhaus, *supra* note 4 (identifying countries with highest number of spam operators). While regulating Dutch-originated spam seems to be well within the Dutch power, eradicating foreign spam appears to be beyond the ability of a single country alone. *See infra* Part III.B.3 (discussing need for international cooperation to eradicate spam problem).

137. *See* Oriola, *supra* note 75, at 126-29 (explaining disconnect between spatial reality and internet reality).

138. *Id.* at 129-30 (describing attempts by courts to apply personal jurisdiction tests to internet interactions).

139. *Id.* at 130 (discussing potential for confusion when attempting compliance with individual state spam laws).

140. *See id.* (explaining difficulty determining geographic location of e-mail address owners). When one

might satisfy proponents of stricter spam legislation than the CAN-SPAM Act provides, it is essentially forcing national compliance of laws on people who have no democratic recourse whatsoever in instances where they are not even interacting with citizens of the state in which it is enacted.[141]

The CAN-SPAM Act does preserve a role for the states, but, because a state must act within the confines of a federally enacted statute, the aforementioned dangers are not present.[142] States, except where acting as ISPs, may only legislate on spammers' fraudulent practices.[143] The statute prevents an individual state from setting the national spam policy, but leaves the states a role in the regulation of spam.[144]

b. Small Differences Between EU Member State Laws Make Problems for Compliance

Despite a rather straightforward provision in the E-Privacy Directive, there is enough variation among the versions of spam regulation enacted by the member states to cause difficulties.[145] The EU insisted each member state enact a statute embodying the general provisions of Article 13.[146] It did not, however, seem particularly concerned with variations in the specifics of the legislation.[147] This consequence is more likely to affect a legitimate business attempting to comply with European law than a spammer employing deceptive practices.[148] A spammer sending fraudulent UCEs certainly would not care if she was in compliance with the Directive, whereas a business attempting to navigate the exception could face serious consequences due to accidental violations.[149]

---

is sending UCEs to thousands or even millions of people, it would be crippling to have to go through the entire list and determine one by one where each person is located. *See* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 356 (4th Cir. 2006); *see also* Oriola, *supra* note 75, at 121 (describing practice of spammers buying CDs containing millions of e-mail addresses). As a result, to protect him or her self, the sender would simply have to comply with the strictest of the statutes. *See Omega World Travel*, 469 F.3d at 356.

141. *See supra* notes 68-70 and accompanying text (describing congressional concerns with compliance issues when states enact differing spam policies).

142. *See* 15 U.S.C. § 7701(b)(1) (2006) (permitting states to prohibit falsity or deception); *see also Omega World Travel*, 469 F.3d at 355 (holding OK law not preempted because within CAN-SPAM exception to preemption).

143. *See supra* notes 76-80 and accompanying text (explaining state legislative power limited to material misrepresentations and fraudulent practices).

144. *See supra* notes 71-72 and accompanying text (explaining remaining role for states); *supra* notes 139-140 and accompanying text (describing problems when only states legislate spam law).

145. *See supra* notes 109-115 and accompanying text (explaining Article 13 and selective member state enactment).

146. *See* Hart, *supra* note 126, at 565 (describing EU action responding to poor member state compliance).

147. *See generally Communication on Fighting Spam*, *supra* note 129, at 12 (focusing on lack of consistency in enforcement over statutory variations).

148. *See* Delaney, *supra* note 109, at 125-26 (describing myriad inconsistencies between laws of various member states).

149. *See* supra notes 113-115 and accompanying text (explaining potential pitfalls in EU member state law for unwary businesses).

2. The Importance of ISP Autonomy

If the CAN-SPAM Act had preempted ISPs' action against legalized UCEs, it would have left individuals and businesses completely unprotected and open to flooding by all UCEs that are now generally blocked.[150] It would be almost impossible for an ISP to wade through thousands or millions of potential spam e-mails traveling through its system to determine which were compliant and which were not.[151] Additionally, spam not in compliance with the statute might be difficult to find because spammers can disguise spam that violates the Act to appear compliant.[152] Accordingly, leaving the ISPs with discretion to deal with UCEs is an important feature.[153]

3. Do-Not-E-mail Registries

The call for a Do-Not-E-mail registry has essentially passed, and there is no longer encouragement for its use.[154] Indeed, such registries, if found by unscrupulous spammers, serve only to provide a list of legitimate e-mails invaluable to any spammer.[155] Nothing has ever been done to create such a registry either in Europe, pursuant to the E-Commerce Directive, or in the US, pursuant to section 7708 of the CAN-SPAM Act.[156]

4. Distinguishing Natural and Legal Persons

The distinction between natural and legal persons is one of the most problematic features of the E-Privacy Directive.[157] There is ample evidence of the huge cost of spam to businesses.[158] The cost is probably even greater to a

150. *See Spam Experiment Overloads Inboxes*, *supra* note 3 (explaining that without spam filter and protection UCEs flooded inboxes).

151. *See* Kleiner, *supra* note 3 (estimating total of 120 billion spam e-mails sent per day). With spam e-mail constituting eighty or ninety percent of e-mails sent worldwide, an ISP simply would not have the time or the resources to sort through them to determine which are compliant. *See id.*

152. *See* 15 U.S.C. § 7704 (2006) (setting forth requirements for compliant e-mail); *see also* Soma, *supra* note 55, at 179 (describing difficulty proving every UCE sent by spammers noncompliant with CAN-SPAM).

153. *See supra* notes 150-152 and accompanying text (explaining danger of blocking ISP action).

154. *See, e.g.,* Soma, *supra* note 55, at 183-84 (explaining FTC decision that Do-Not-E-Mail registry too vulnerable to abuse); Bambauer, *supra* note 51, at 77 (stating FTC chairman "would not sign up for" registry due to danger of abuse) (internal quotations omitted); Magee, *supra* note 90, at 367 (noting public opt-out list in Europe "might actually do more harm than good") (internal quotations omitted). Further proof of the potential for abuse arose shortly after the passage of the CAN-SPAM Act, when spammers created a fake Do-Not-E-Mail registry to harvest legitimate e-mails. *See* Soma, *supra* note 55, at 184.

155. *See* Soma, *supra* note 55, at 184.

156. *See* E-Privacy Directive, 2002 O.J. (L 201) 37 (EC) (lacking provision for registry); Soma, *supra* note 55, at 184 (describing FTC decision not to create registry). In the United States, due the potential dangers of Do-Not-E-Mail registries, the FTC abandoned the concept as a potential weapon against spam. *See* Soma, *supra* note 55, at 184. In Europe, such a concept is no longer necessary because people must opt-in for UCEs. *See* E-Privacy Directive, art. 13(1), 2002 O.J. (L201) 37 (EC).

157. *See supra* notes 116-122 and accompanying text (discussing EU decision for discretionary distinction between natural and legal persons and its perils).

158. *See supra* notes 2-8 and accompanying text (describing toll spam e-mail takes on businesses).

business because, while a person is merely frustrated, a business loses money for every minute spent by an employee dealing with spam.[159] Though most member states chose to enact the opt-in policy for both natural and legal persons, there were those that chose to differentiate between the two.[160]

5. European Opt-In vs. United States Opt-Out

The most significant benefit of an opt-in over an opt-out policy is the ease of enforcement.[161] In an opt-in system, simply by finding UCE in someone's e-mail inbox, the sender has violated the statute provided the message does not fit into an exception.[162] Thus, when bringing an action against the sender, the burden to show a violation for each e-mail sent is not very great.[163] However, in an opt-out system such as in the CAN-SPAM Act, the person seeking to bring an action against the sender would have to examine each e-mail in detail to determine if it was in violation of the Act.[164] This is a heavy burden of proof considering the number of messages generally involved in spamming.[165] That being said, the burden is not so overwhelming that government action using the CAN-SPAM Act is impossible.[166]

It is not clear whether opt-in systems have a higher rate of successful deterrence. Spammers will likely take action to avoid being affected by statutory schemes they cannot legally overcome.[167] Actions brought pursuant to an opt-in system against people attempting to comply with its terms are fairly easy to prosecute.[168] However, the real problem would likely fall with concealed spammers, who are no easier to find under an opt-in or opt-out regime.[169] If the majority of spam comes from people seeking to conceal their

159. *See supra* notes 2-8 and accompanying text (summarizing cost of spam to businesses).

160. *See* ITU SURVEY, *supra* note 120, at 47 (describing Portuguese anti-spam legislation applying opt-in to natural persons only); Kikuchi, *supra* note 109, at 302 (noting UK also chose to differentiate between legal and natural persons). Even one country that formerly chose to distinguish between businesses and natural persons has recently acknowledged the mistake of that decision, and is moving to change its law to include businesses. *See Netherland's Spam Law Expands*, *supra* note 2 (reporting change of law in Netherlands).

161. *See* Soma, *supra* note 55, at 180-82 (suggesting easier to enforce ban on all unsolicited commercial e-mail).

162. *See supra* part II.B.3.a (explaining EU opt-in).

163. *See* Soma, *supra* note 55, at 181 (arguing straightforward definition of spam leads to easier identification and enforcement).

164. *See* 15 U.S.C. § 7704 (2006) (containing maze of requirements for illegal spam); *see also* Soma, *supra* note 55, at 179 (explaining first must find spammer, then show each of e-mails violates CAN-SPAM Act).

165. *See supra* note 3 and accompanying text (estimating around eighty percent of all e-mail is spam).

166. *See generally* United States v. Kilbride, 507 F. Supp. 2d 1051, (C.D. Ariz. 2007) (representing successful government action pursuant to CAN-SPAM).

167. *See* Baxter, *supra* note 50, at 175 (stating spammers expanding overseas in response to increased regulation). Additionally, spammers who employ deceptive practices become extremely difficult to find, let alone prosecute. *See* Soma, *supra* note 55, at 179.

168. *See supra* notes 161-165 (describing advantages to enforcement under opt-in system)

169. *See* Soma, *supra* note 55, at 179 (noting one spammer concealed "among a throng of spammers working off a maze of ISPs").

identities, then neither system seems to have much of an advantage over the other.[170]

One problem with an opt-out system that does not involve enforcement is that opt-out mechanisms can ultimately end up as a valuable tool for spammers. The opt-out system is supposed to provide a safe way for recipients to stop companies from sending them legitimate e-mail advertising, should the e-mail user so choose.[171] However, the opt-out links can actually help spammers identify active targets for additional UCEs by confirming which addresses belong to actual people.[172]

B. Suggestions for the Future

Ultimately, UCEs are an attractive marketing device because they provide a relatively easy way to reach huge numbers of consumers at a relatively low cost.[173] As long as that balance remains, it is likely countries will continue to fight a losing battle. Accordingly, the goal of any effective anti-spam action must be either to shift the cost back to the spammer, or to make it a less efficient way to reach people.

1. Private Cause of Action

One way to shift costs is to allow private plaintiffs, other than ISPs, to have a right of action against spammers.[174] It has even been suggested that private rights of action for individuals could create "a self-sustaining anti-spam system that provides a means for individuals to seek recourse without having to rely on ISPs, state attorneys general, and government agencies for enforcement."[175] The main problem with this kind of solution is the same one that plagues seemingly every potential solution: it is difficult to locate spammers, and they often move into jurisdictions where they are unreachable.[176] A private right of action will only be effective against spammers who are caught and found liable.

---

170. *See supra* notes 167-169 (noting common problem in both opt-in or opt-out systems).

171. *See supra* notes 53-55 and accompanying text (explaining opt-out requirement and suggesting Act meant to allow legitimate UCE).

172. *See* Sullivan & De Leeuw, *supra* note 43, at 895-96 (describing unscrupulous use of opt-out links by spammers).

173. *See* Oriola, *supra* note 75, at 121-23 (explaining how spam functions). One computer is capable of sending 650,000 e-mails per hour, adding up to staggering numbers in one day from a single spammer. *Id.* at 123. The main cost for a spammer is gaining access to e-mail addresses. *See id.* Apparently, even that is not a particularly difficult task as there are companies who sell CDs that can reportedly contain over 90,000,000 addresses. *See id.* at 121.

174. *See* Soma, *supra* note 55, at 193-95 (suggesting private rights of action for individuals an effective means of enforcement). In 2008, the European Data Protection Supervisor, Peter Hustinx, said that the E-Privacy Directive should be amended to allow individuals to bring class action lawsuits under the Directive. *See* Mitchell, *supra* note 109, at 576 (setting forth Hustinx's views on the Directive).

175. *See* Soma, *supra* note 55, at 194-95.

176. *See supra* Part III.A.5 (determining problem with opt-in and opt-out is catching spammers and holding them accountable).

2. Increased ISP Involvement

John Soma, Patrick Singer, and Jeffrey Hurd presented an intriguing solution in an article they coauthored entitled *Spam Still Pays: The Failure of the Can-Spam Act of 2003 and Proposed Legal Solutions*.[177] They suggest creating ISP liability for facilitating the sending of spam, but only to other ISPs, could create a very effective solution to spam e-mail.[178] It seems ISPs might be in the best possible situation to aid in the fight against spam.[179] Because of their unique positions, ISPs have much more knowledge and understanding about spammers, and if given a motive, might be able to do a great deal to prevent spam from being transmitted.[180] This solution, unlike private causes of action to individuals, avoids the issue of hidden spammers because the ISPs involved are easy to locate.[181]

3. International Cooperation

Regardless of the method ultimately used in the fight against spam, one thing is certain: there must be international cooperation if there is to be any hope for success.[182] As countries become more successful in their efforts to prevent spam e-mail, spammers will continue to move their operations to countries whose policies are more hospitable.[183] Ultimately, without international cooperation, it is unlikely any attempt at preventing spam will be successful.[184]

---

177. *See* Soma, *supra* note 55.

178. *See* Soma, *supra* note 55, at 186-93 (explaining disincentive for ISPs action but arguing creating ISP liability could encourage better spam prevention). Spam e-mail must originate from an ISP in order for it to be sent. *See id.* at 191-93. Additionally, the cost of e-mail transmission to the ISP is as low as that for the spammers themselves. *See id.* at 192. In addition, the ISPs benefit to a certain extent from spamming because they can market their spam-fighting tools to attract more customers. *See id.*

179. *See id.* at 186-93 (explaining relationship between ISP and spammers and reasons they could help solve spam problem).

180. *See id.* at 191 (describing potential profit from inaction versus stricter attempt blocking spam potentially resulting in customer dissatisfaction). As it stands, an ISP might face greater consequences from attempting to block spam than it would from doing nothing. *See id.* Nevertheless, changing that balance might lead to a more comprehensive solution to spam because ISPs are much closer to the source and can deal with the problem in a way no one else can. *See id.*

181. *See id.* at 191 (explaining limited number of ISPs make bringing action routine).

182. *See infra* notes 183-184 and accompanying text (explaining necessity of worldwide cooperation). Even Congress and the FTC have acknowledged the need for more international cooperation in the fight against spam and other internet based threats. *See* THE FTC REPORT ON SAFE WEB, *supra* note 62, at 1; *see also supra* notes 61-62 (describing SAFE WEB and progress in FTC enforcement using international cooperation). In its report, the FTC also stated it is currently in the process of negotiating and drafting agreements with Canada and the European Commission that would further strengthen the international cooperation between the countries. *See* THE FTC REPORT ON SAFE WEB, *supra* note 62, at ii.

183. *See* Soma, *supra* note 55 at 195 (stating spammers will move to other countries as anti-spam laws become stronger and more effective).

184. *See e.g. Communication on Fighting Spam*, *supra* note 129, at 4 (describing spam as a "cross-boarder issue"); ITU SURVEY, *supra* note 120, at 62 (stating "international cooperation . . . [is] indispensable"); Oriola, *supra* note 75, at 166 (explaining necessity of worldwide effort to effectively control spam).

IV. CONCLUSION

Currently neither the U.S. nor the EU legal system has really discovered the solution to the spam problem. The United States' attempt at curbing spam through the CAN-SPAM Act has clearly failed in significant ways, as the United States is the number one outsourcer of spam e-mail worldwide. Although the European Union has seen some limited success in its attempts to curb spam, it still faces many of the same problems as the United States. Whatever the future solution may be, it seems clear that ISPs must be given the ability to place additional controls and filters on the messages flowing through their servers, and the CAN-SPAM Act correctly preserved that control. As for the European Union Directive, the only way for anyone to begin successfully combating spam is for the rules to be enforceable against all spammers, not just the legitimate businesses. While it is not clear an opt-in system can actually deal with all the problems of spammers, there is at least an ease of enforcement. Meanwhile, it has become clear that enforcement under an opt-out system is much more complicated: each e-mail has to be sorted through and proven to be in violation.

The ultimate failure of these anti-spam systems is not necessarily one of structure: individual governments alone, even a group of treaty countries working ostensibly together, do not have the power to combat the problem on their own. Spammers have become too sophisticated and too widespread for countries to eradicate spamming entirely. The only real way to stop spam e-mailing is to have a worldwide, integrated system including countries, ISPs, individuals, and law enforcement agency cooperation. Collectively, they must make spam a less attractive marketing tool than it currently is. Without imposing high costs on spammers or reducing the potential reach of spam, it will never disappear as an attractive advertising tool.

Ariella Mutchler