Article

An Analysis of Institutional Choices in Regulating Internet Spam

Chia-Li Shih *

ABSTRACT

The Internet has created a channel that allows for the rapid dissemination of information without regard to geographical boundaries. Unsolicited commercial e-mail ("UCE"), or "spam" as it is commonly known, is generated from enormous lists of e-mail addresses for the purpose of sending commercial information without seeking the e-mail account holder's permission. Spam capitalizes on the unique nature of the Internet to engage in direct marketing in the fastest and most efficient way currently possible. Nevertheless, UCEs come with significant negative external costs. Furthermore, spam raises global legal issues in the areas of cyberspace privacy and security.

This article approaches this topic by employing a law and economics analysis to identify appropriate institutional choices necessary for the regulation of UCEs. By comparing the legal frameworks of the United States, the European Union and Japan, this article evaluates the effectiveness of different legal approaches and proposes an international legal framework for cooperation in regulating UCEs.

Keywords: *Unsolicited Commercial E-mail, Spam, Institutional Choice, Can Spam Act, Direct Marketing, Law and Economics*

DOI：10.3966/181263242015091002002

* The author is currently an assistant professor of Tunghai University, College of Law. She obtained her Doctor of Juridical Science (S.J.D) from University of Wisconsin, at Madison. She is admitted to bars of the State of California and New York and is an experienced US attorney. Professor Shih's research and practice primarily focuses on electronic commerce law including electronic payments and electronic transactions and also cross-border litigation.

CONTENTS

The Internet has created a channel that allows for the rapid dissemination of information without regard to geographical boundaries. However, new technologies not only bring with them great benefits but also often unforeseen problems. Unsolicited commercial e-mails ("UCE"), or "spam" as it is commonly known, is generated from enormous lists of e-mail addresses. Commercial information is sent directly to e-mail addresses without seeking the account holder's permission. Spam capitalizes on the Internet's ability to rapidly disseminate information for the purpose of engaging in direct marketing in the fastest and most efficient way currently possible.

Although UCEs can be appreciated as a cost-effective means of advertising commercial products and services, they also have a negative impact. Specifically, UCEs come with significant external costs and create global legal issues in the areas of cyberspace privacy and security.

This article discusses this issue by employing a law and economics approach to analyze the costs and benefits of UCEs and then identifies the appropriate institutional choices necessary for the regulation of UCEs. Specifically, this article compares the legal frameworks of the United States, the European Union and Japan. By comparing and evaluating the effectiveness of different legal approaches, this article proposes an international legal framework to promote and establish the foundation for international cooperation in regulating UCEs.

I. BENEFITS AND COSTS OF UCES

UCEs are a cost-effective means to communicate with a wide range of potential transactional parties. The low costs associated with simultaneously sending copious commercial advertisements to potential consumers via e-mail dramatically decreases businesses' transaction costs such as marketing expenses. Given this advantage, UCEs help to decrease entry barriers for businesses, which increases competition – a benefit often thought of as bestowing a positive effect on the market. This low cost encourages businesses to adopt the use of UCEs in order to boost their market share.

However, UCEs can and do harm consumers and Internet service providers ("ISPs"). Furthermore, the increased competition and boosts in market participation resulting from UCEs create a risk of market failure. It is indisputable that UCEs, by their very nature, are a double-edged sword. Therefore, this section will identify the tipping point between the costs and benefits of UCEs.

A. *Benefits of UCEs*

Marketers have different methods available to them to market their goods and services. Some of the traditional marketing methods include mailing catalogues, flyers and coupons. Marketers also rely on print media, and more recently, telemarketing via phone and fax. UCEs are a new type of direct marketing. They have a number of advantages over conventional marketing channels due to their quick, inexpensive and efficient nature.[1] Millions of UCEs can be sent to a wide range of potential consumers simultaneously. More significantly, increasing the number of recipients only increases the cost to the senders by an extremely marginal amount. This suggests that there is an inherent incentive to maximize the number of UCEs sent. Compared to conventional direct marketing tools such as telemarketing or direct mailings, UCEs, on a per recipient basis, are extremely cost effective marketing tools. Given that an enormous volume of UCEs can be sent simultaneously, even a low return rate can make spamming a profitable and effective tool to reach out to a substantial numbers of potential customers.[2]

As a more efficient marketing tool, UCEs provide businesses and the market as a whole two important benefits: significantly decreased transaction costs and reduced entry barriers to the market.

1. *Decreased Transaction Costs*

A comparison between UCEs and conventional telemarketing shows that UCEs significantly decrease the costs of each direct commercial message. Phone telemarketer utilizes a technology called automatic dialing-announcing devices ("ADAD"),[3] which automatically dials a long list of phone numbers and plays pre-recorded advertisements. The cost for this marketing model is the total cost of dialing each phone call. In terms of the volume of phone calls made, ADAD can dial up to one thousand five hundred (1,500) calls per day. If a local business phone line with unlimited minutes costs USD 45 per month, the cost for each call is 0.1 of a cent.

Comparatively, if a business utilizes UCEs as a marketing tool, the cost of marketing is significantly lower. Specifically, the cost to send 3.5 million UCEs is roughly USD 350. The base cost for each e-mail is then $350

---

1. Lily Zhang, *The CAN-Spam ACT: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L. REV. 301, 303 (2005).

2. 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).

3. Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 374 (2000).

divided by three million five hundred thousand messages, which is one hundred-thousandths of a cent (USD 0.0001) per e-mail.[4] Therefore, the cost of using telemarketing is significantly higher than using UCEs. In addition, other factors such as "do-not-call" lists in the United States and Canada represent a significant drawback to the effectiveness of telemarketing campaigns compared to UCEs.[5]

In addition to the lower costs, UCEs are also more effective than ADAD because they can reach a wider range of potential customers, not only in terms of the sheer number of customers but also in terms of geographical areas covered on the account of the borderless nature of the Internet.

2. *Decreased Market Entry Barriers and Increased Competition*

UCEs also decrease the barriers to market entry and increase competition. Conventional economic models suggest that lower marketing costs will translate into lower product prices and result in better competitiveness.[6]

Specifically, transaction costs have a significant impact on the parties' ability to proceed with a contractual relationship. Transaction costs are defined as the "resources necessary to transfer, establish and maintain property rights."[7] Typical examples of transaction costs are information costs, search costs, the costs of meetings, negotiations and all other costs incurred in order to conduct transactions.[8] UCEs decrease these transaction costs by providing means to market a product with minimal marketing expenses. Lowering the transaction costs creates a low entry barrier in a particular commercial environment, thereby allowing smaller businesses to participate in a market. Furthermore, the market as a whole will become more competitive due to the presence of multiple players. In other words, small businesses can gain more potential consumers at lower cost, which

---

4. Sameh I. Mobarek, *The Can-Spam Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to It?*, 16 LOY. CONSUMER L. REV. 247, 248 (2004).

5. The Telemarketing and Consumer Fraud and Abuse Prevention Act grants the Federal Trade Commission (FTC) authority to enforce and prescribe rules prohibiting deceptive telemarketing acts or practices. 15 U.S.C. § 6101-6108 (1994). The FTC enacted rules governing telemarketing sales methods and established a "national do not call registry." 16 C.F.R. § 310 (2010). Consumers who do not want to receive calls from telemarketer can register their phone number on the list. Once consumers have registered, telemarketers have up to 31 days from the date of the registration to stop calling registered consumers; *see also* https://telemarketing.donotcall.gov/.

6. MARGARET J. RADIN ET AL., INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORKS 941 (2002).

7. RICHARD O. ZERBE JR., ECONOMIC EFFICIENCY IN LAW AND ECONOMICS 168 (2001).

8. *See, e.g.*, JEFFREY L. HARRISON, LAW AND ECONOMICS IN A NUTSHELL 62 (1995); Robert C. Ellickson, *The Case for Coase and Against* "*Coaseanism*", 99 YALE L.J. 611, 612 (1989) (the author classified transaction costs into three categories based upon functions of transaction costs. These are get-together costs, decision and execution costs, and information costs).

makes it easier to establish a market share and compete with larger entities.[9] By decreasing transaction costs and lowering the entry barriers for businesses, UCEs therefore increase market competition and the availability of goods.

B. *Costs of UCEs*

According to a study conducted by Kaspersky Lab ZAO in the second quarter of 2013, UCEs constituted 70.7 percent of all e-mail traffic.[10] Given that the worldwide e-mail traffic was 507 billion messages per day,[11] this means that 358.4 billion UCEs were sent per day. With UCEs flooding e-mail accounts, consumers, corporations, and ISPs end up bearing the costs associated with processing these commercial messages.

This inherent cost shifting structure of UCE makes it a unique direct marketing tool. With conventional marketing tools, the senders generally bear the costs of advertising. However, UCEs shift these costs to consumers. Ferris Research Report estimated that, in 2005 worldwide cost of UCEs was USD 50 billion. In 2009, the cost ballooned to USD 130 billion.[12] While, UCEs provide positive externalities which lower entry barriers and increase competition in the market, they also create negative externalities by shifting costs on the recipients, decreasing corporate productivity and causing risks of potential market failure. These externalities are analyzed below.

1. *Costs to Individual Consumers*

UCEs impose costs on individual consumers' time and privacy. UCEs flood personal e-mail accounts with irrelevant and voluminous advertisements that overload consumers' accounts. Consumers, in turn, must invest time to delete these messages. The time consumed by deleting UCEs is significant. Research shows that the time spent deleting spam could easily add up to between USD 12 to 20 billion per day in lost productivity.[13] UCEs

---

9. RADIN ET AL., *supra* note 6, at 941.

10. DARYA GUDKOVA, SPAM IN Q2 2013 (2013), https://securelist.com/analysis/quarterly-spam-reports/37148/spam-in-q2-2013/. Kaspersky Lab is an IT security vendor which constantly monitors and researches spam traffic in order to identify and combat IT threats.

11. E-MAIL STATISTICS REPORT, 2009-2013 (Sara Radicati ed. 2009), http://www.radicati.com/wp/wp-content/uploads/2009/05/email-stats-report-exec-summary.pdf.

12. Justin M. Rao & David H. Reiley, *The Economics of Spam*, 26 J. ECON. PERSPECTIVES 87, 98 (2012).

13. *See id*. at 99 (according to the estimate, if we assume only 1.8% to 3% of 50 million UCEs actually reach consumers and each consumer spends 5 second to delete each UCE, and the average value of one hour of time is $25 USD, the total end-user costs will be approximately $12-20 billion per day. If a better spam filter is applied, the costs could go down to $6 billion per day).

also impose additional costs in situations where important messages are missed in the flood of e-mails.[14]

In addition, some UCEs contain malicious programs, which expose computers to virus threats and privacy ricks. The majority of malicious programs are designed to steal personal information, especially financial data, such as online banking information.[15] Moreover, since ISPs expend significant effort implementing and improving spam filtering systems, the costs incurred are ultimately passed on to consumers.[16]

2. *Costs to Internet Service Providers and Corporations*

The costs associated with UCEs amount to significant liabilities to ISPs and corporations. For ISPs, the large numbers of UCEs processed consume server capacity and create additional technical costs related to the maintenance of services. For example, one of the largest ISPs in United States, America Online, Inc. ("AOL") filed a lawsuit against National Health Care Discount Inc. ("NHCD") claiming that NHCD sent one hundred and thirty five million UCEs to AOL's subscribers during the period relevant to the lawsuit. This resulted in repair costs and lost profits.[17] Specifically, AOL claimed that the monetary damages suffered, among other damages claimed, were one hundred and five thousand three hundred dollars (USD 105,300).[18] AOL also alleged that NHCD's costs to send each UCE to AOL's members were as low as seventy-eight hundred thousandths of a cent (USD 0.00078), and therefore NHCD and other spammers would rather pay the calculated damages and "appropriate the use of AOL's equipment without compensating AOL for any profits."[19] The Court agreed with AOL's assertion and granted damages in the amount of three hundred thirty-seven thousand five hundred dollars (USD 337,500).[20]

In addition to the tangible costs suffered by ISPs in expanding hardware capacity to accommodate the huge volume of e-mail traffic, spammers' tortious conduct also results in damage to the reputation of ISPs in terms of their ability to provide secure and reliable service. The impact of UCEs on

14. Dennis W. K. Khong, *An Economic Analysis of Spam Law*, 1 ERASMUS L. & ECON. REV. 23, 32 (2004).

15. GUDKOVA, *supra* note 10.

16. Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 1267 (Cal. App. 1st Dist. 2002).

17. America Online, Inc. v. National Health Care Discount, Inc., 174 F. Supp. 2d 890, 915 (N.D. Iowa 2001).

18. *Id*. at 900 (The court determined two approaches to calculate the damages. First, the damage should be the actual cost of delivering each piece of UCE sent by NHCD to AOL's members. Second, the damage is the cost of delivering at the rate an advertiser would be charged for a "banner advertisement displayed on AOL members' e-mail in-boxes.").

19. *Id*.

20. *Id.* at 901-02.

ISPs also includes a slowdown in Internet traffic. This makes it difficult for ISPs to process legitimate e-mails.[21] Service providers have devoted great efforts to develop and purchase anti-spam technology to build better filtering systems to stop UCEs from reaching e-mail account holders. According to Ferris Research, in 2009 it was estimated that the cost of anti-spam technology in the United States was approximately USD 6 billion per year.[22]

In the corporate sector, in order to avoid exposure to viruses and decrease the huge volume of UCEs that overload e-mail systems, corporations are incorporating anti-spam technology into their e-mail systems. For example, Yahoo! Mail spends approximately USD 55 million per year in anti-spam technology to cover its 500 million e-mail accounts.[23]

Nevertheless, spam remains a moving target for web security companies. According to a 2014 Cisco report, despite the efforts and developments in spam filtering technology, the average number of UCEs sent per month reached 200 million messages during the last three years. This amount is almost double of the normal levels of UCEs sent.[24] One of the reasons for this increase is tied to the relative success of companies in fighting spam. Realizing that no filtering system is perfect, UCE senders increase the numbers of messages sent in order to boost the chance of their UCEs passing through various filtering systems. Thus, while various filtering systems are in place, they must be constantly updated and maintained to filter out oceans of spam messages.

In addition to these costs, UCEs also decrease user productivity. According to a study conducted by Nucleus Research, Inc., UCEs cost the US businesses an estimated USD 71 billion in lost productivity or approximately USD 712 per employee per year.[25]

3. *Potential Market Harm*

UCEs help to decrease transaction costs by lowering marketing costs, entry barriers, and also increase market competition. However, UCEs may also promote unsound competitive advantages over legitimate merchants. By using UCEs as a tool to advertise without complying with relevant regulations, such as obtaining the recipients' consent, there is a significant reduction in the transaction costs associated with marketing a product through commercial e-mails.

---

21. Verizon Online Services, Inc. v. Ralsky, 203 F. Supp. 2d 601, 604 (E.D.Va. 2002).

22. Rao & Reiley, *supra* note 12, at 100.

23. *Id.*

24. Jaeson Schultz, *Spam Hits Three Year High-Water Mark*, CISCO BLOGS (May 2, 2014), http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark.

25. Ariella Mutchler, *Can-Spam Act Versus the European Union E-Privacy Directive: Does Either Provide a Solution to the Problem of Spam*, 43 SUFFOLK U. L. REV. 957, 958 (2010).

As described in Gresham's Law, unsound competition can cause market harm and lead to market failure.[26] This can be demonstrated in a hypothetical scenario involving Merchants A and B. Both are selling an identical product with a base cost of ten dollars ($10).

Merchant A promotes the product by sending out UCEs. The total cost of marketing the product for Merchant A is one dollar (USD 1). Merchant B, however, promotes the product by posting ads on websites and uses traditional media, such as television, radio, telemarketing and newspapers. Marketing costs per product to Merchant B are five dollars (USD 5). If we calculate the selling price based on a twenty percent (20%) profit, the selling price for Merchant A will be thirteen dollars and twenty cents (USD 13.20) and eighteen dollars (USD 18) for Merchant B. This calculation is summarized in Table 1 below:

Table 1: Unfair Commercial Advantage

	Merchant A	Merchant B
Base Costs	$10	$10
Marketing Costs	$1	$5
Total Cost	$11	$15
Sales Price (incl. 20% profit)	$13.2	$18

(Table was generated by the author.)

By realizing significant savings in marketing costs, Merchant A can sell the same product at a lower price than Merchant B. In addition, UCEs allow Merchant A to reach a wider range of consumers, thereby increasing his/her customer base. Thus, Merchant A can gain a competitive advantage over Merchant B.[27] Over time, Merchant A can gain a greater market share than Merchant B, who will eventually leave the market because he/she cannot compete with Merchant A's prices.

The increased competition created by UCEs also increases the risk of market failure. First, spam is an unsound commercial practice as it shifts its costs to consumers and ISPs.[28] Businesses that utilize sound practices, such as in the scenario described above, cannot gain market share and are unable to compete. Eventually, bad commercial practices will survive with continued price competition among the remaining companies.[29] In the end,

26. LOUIS PHLIPS, THE ECONOMICS OF PRICE DISCRIMINATION 239 (1983).

27. MUKUL PANDYA, ROBBIE SHELL, SUSAN WARNER, SANDEEP JUNNARKAR & JEFFREY BROWN, NIGHTLY BUSINESS REPORT PRESENTS LASTING LEADERSHIP: WHAT YOU CAN LEARN FROM THE TOP 25 BUSINESS PEOPLE OF OUR TIMES 132 (2004) (it is a typical practice for companies to manage costs in order to lower price in order to gain competitive advantages).

28. Missouri ex rel. Nixon v. American Blast Fax, Inc., 323 F.3d 649, 654 (8th Cir. 2003).

29. This is called "Gresham's Law." George A. Akerlof, *The Market for Lemon: Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 490 (1970).

profits will be so low that sound and unsound businesses alike will not be able to survive.

Second, misuse of UCEs also gives rise to the free-rider problem that creates unfair competition. For example, in the case of America Online, Inc. v. LCGM, Inc., LCGM targeted AOL's members and used AOL's trademarks in their e-mail headers in connection with advertisements.[30] Misusing AOL's name caused confusion among AOL's members because spammers created an impression that AOL had sponsored LCGM's products.[31] LCGM not only diluted AOL's marks but also took a free ride on AOL's efforts to establish a distinctive trademark and commercial reputation. In addition, such practice also allows for illegal activities such as phishing. By masquerading as a trustworthy entity, the UCE contains a link to malware in order to acquire personal information, such as credit card information, account user names, passwords etc. Thus privacy concerns involving identity theft have become a major obstacle to the growth of ecommerce.[32]

II. PROPER INSTITUTIONAL CHOICE TO MAXIMIZE THE BENEFITS OF UCES AND MINIMIZE THEIR COST

Having analyzing the benefits and costs of UCEs, the goal of this article is to find a solution that can maximize the benefits and minimize the costs of UCEs. Decreasing transaction costs can only have a positive impact on the market when a sound transactional environment is established and maintained. By exploring the benefits of decreasing the transaction costs from UCEs and avoiding the cost shifting problem to end-user, this article looks to find a proper institutional choice to reach the goal of resource allocation efficiency while avoiding the risks of market failure present in the current environment.[33]

A comparative analysis of institutional choices should evaluate the

30. America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 449 (E.D.Va. 1998).

31. The court found that LCGM violated 15 U.S.C. § 1125 (a) (1) of the Lanham Act. The elements necessary to establish a false designation violation under the Lanham Act are: (1) a defendant used a designation; (2) in interstate commerce; (3) in connection with goods and services (4) which designation is likely to cause confusion, mistake, or deception as to origin, sponsorship, or approval of defendant's goods or services; and (5) plaintiff has been or is likely to be damaged by these acts. *See e.g.*, *id*.; First Keystone Federal Saving Bank v. First Keystone Mortgage, Inc. 923 F. Supp. 693, 707 (E.D.Pa. 1996).

32. IDENTITY THEFT 60 (Claudia L. Hayward ed., 2004).

33. NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 4, 14 (1994) (professor Komesar further explained the concept of "resource allocation efficiency." "Resource allocation efficiency focuses on the balance of social costs and benefits. As it is used in legal analysis, concern for resource allocation efficiency is often seen in judicial balancing of these aggregate impacts. More precisely, resources are most efficiently allocated when they go to the use for which they are most demanded.").

effectiveness of each decision-making process.[34] The three primary institutional choices for responding to the challenges posed by UCEs are the market, the political process and the adjudicative process. By comparing and analyzing different institutional choices and their impacts on social policies, we can identify the most appropriate mechanism that can balance the costs and benefits of UCEs and further resolve the issues caused by spam, thereby best achieving the efficient allocation of resources.[35]

A. *Market*

The goal of every economic system is to make the market participants better off by providing sufficient options and allocating resources efficiently.[36] Since the time of Adam Smith, "market" has been viewed as a powerful mechanism for the allocation of resources.[37] Through the interactions between the market's participants, the assumption is that self-interest in a free market regulated by the "invisible hand" will balance supply and demand, thus maximizing the efficiency of resource allocation.

However, given that it is implausible for any market to be truly free, different transaction and information costs involved in exchanges produce a variety of aggregated results.[38] Furthermore, the market as an institutional choice is unique, given that it lacks a central authority. It is simply a process of aggregated results and interactions between participants through setting prices and outputs, allocating society's resources, distributing wealth, and determining opportunities.[39]

As the market focuses on the process and results of the interaction between market participants, the evaluation of the market's effectiveness should adopt the participation-centered approach and therefore take different patterns of participation into account in order to fairly evaluate if the market itself can produce an efficient resource allocation and fair distribution.[40] In evaluating the effectiveness of the market as a proper institution to regulate UCEs, there are two significant factors that show different participation patterns in the UCEs practices from conventional marketing tools that must be taken into consideration. The first major factor is the unsound practice caused by sending UCEs illegally and the second is the impact of cost-shifting imposed by UCEs.

---

34. *Id*. at 3.
35. A. Brooke Overby, *An Institutional Analysis of Consumer Law*, 34 VAND J. TRANSNAT'L L. 1219, 1231 (2001).
36. EDWIN MANSFIELD, MICRO-ECONOMICS: THEORY AND APPLICATION 10 (5th ed. 1985).
37. ADAM SMITH, THE WEALTH OF NATIONS (1911).
38. KOMESAR, *supra* note 33, at 98.
39. *Id.*
40. *Id.* at 99.

The costs-shifting effects of UCEs cause negative externalities on the market. An externality is defined as an "effect on a specific market, the source of which is external to this particular market."[41] A negative externality embodies expenses resulting from the market participant's activities that the market participant does not internalize and instead imposes on others. These effects are external because there are derivative costs arising out of activities of the market participant without transactions to represent them. Externalities, by their nature, represent failure to participate, which is generally referred to as a market malfunction or a market failure in traditional welfare economics.[42]

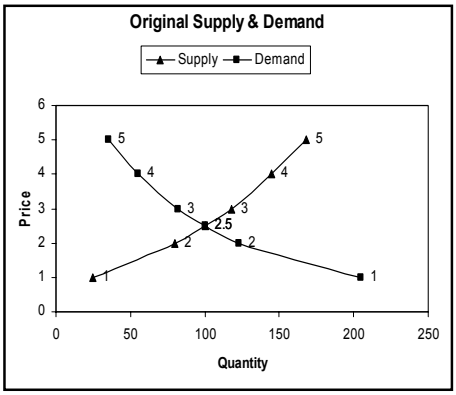
As was highlighted above, spamming is an activity that creates negative externalities. Spammers significantly decrease transaction costs for themselves, but their actions shift the costs to ISPs and consumers. The externalized costs manifest themselves in terms of the costs associated with developing filtering systems and increasing hardware capacity. Furthermore, there is a significant loss in productivity in terms of both, hardware system resources and manpower time spent deleting UCEs. Due to their drive to gain a competitive advantage within their market, spammers seek out the ways of externalizing these costs onto others (i.e. internet service providers or computer users). In contrast, from the computer users' perspective, a significant social benefit of resolving the spam issue through transacting (i.e. market interaction) is divided among hundreds of millions of users, thereby significantly reducing the per capita benefits to be gained from transacting through market institutions.[43] Moreover, there is a high possibility that general computer users might not even recognize the benefits of transacting to address the spam issue or the cost of negotiating a decrease in externalities caused by spam thereby reducing their individual incentive to participate. Therefore, the lack of participation could mean that the market is an inefficient institutional choice. Where the market equilibrium does not function in a way to maximize welfare or social utility, the self-interest of market participants will lead to unethical practices, increasing the likelihood of market failure.[44]

The following scenario provides another reasoning as to why market failure could be caused by UCEs. Generally, as the market equilibrium is reached through the interaction between the forces of supply and demand, the tug-of-war will eventually provide sufficient profit margins to the supply side, while at the same time satisfying the needs of the demand side. Therefore, resources will be allocated to the person who values them the

41. NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE 79 (2004).
42. KOMESAR, *supra* note 33, at 102.
43. *Id*.
44. ELKIN-KOREN & SALZBERGER, *supra* note 41, at 79.

most. We begin by assuming that the price of one particular product is $5, which includes the costs of manufacturing, advertising, marketing, and a profit margin for the supplier. Assuming this price range, there will be thirty-five consumers demanding the product with one hundred sixty-eight suppliers willing to supply it at that price. As the price of the product goes down, the incentive for consumers to purchase it increases. Therefore, as shown in Table 2 below, lower price is correlated with higher demand. In contrast, lower price will result in fewer suppliers willing to supply the product. After the tug-of-war between the forces of supply and demand, the market will reach an equilibrium where the price is at two dollars and fifty cents.

Table 2: Supply and Demand Equilibrium



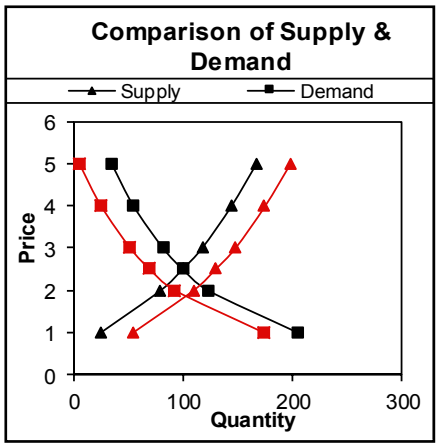
Price	Demand	Supply
5	35	168
4	55	145
3	82	118
2.5	100	100
2	123	80
1	205	25

(Table was generated by the author.)

If we add UCEs into the equation, spam can decrease transaction costs for the supply side. By decreasing the costs of promoting the product to a wider range of potential buyers, there will be more suppliers providing the product at a cheaper price. However, the costs are in fact shifted to the demand side. Thus, consumers bear the costs associated with the use of UCEs, including the costs of protecting privacy and online security, installing and maintaining Internet infrastructures, and developing filtering systems to prevent the problems caused by UCEs. As a result, the market equilibrium will change. Returning back to the scenario outlined above, although the price of the product will remain at 5 dollars, the savings derived through the use of UCEs will translate into a higher number of suppliers being able to supply the product. However, due to this cost-shifting practice, the cost to obtain the product as a whole to consumers is higher, and there will be fewer consumers who can afford to purchase the product at $5. The new market equilibrium will be reached at a lower price of one dollar and

seventy cents, as shown in Table 3 below in grey lines.

Table 3: Comparison of Supply & Demand



Price	Demand	Supply
5	5	198
4	25	175
3	52	148
2.5	70	130
2	93	110
1	175	55

(Table was generated by the author.)

This scenario shows that UCEs can lower the market price for a product and increase market competition because lower transaction costs can attract more competitors. As the price of a product drops, competitors with sound commercial practices would have to sacrifice a part of their profit margin in order to compete. Eventually, the price will become so low that "good" competitors will be driven out of the market. This, in turn, will result in market failure.

In addition to the unsound competitive advantages gained by utilizing UCEs described in the scenario above, the negative externalities created by UCEs' cost-shifting effects also increase the probability of market failure. Traditionally, territorial rules are used to identify externalities.[45] Under this analytical model, a social unit should be defined in order to serve as a base to calculate the externalities and evaluate the effective measure to internalize the costs.[46] The social unit is generally defined by geographic boundaries or jurisdiction, often in terms of national governments providing a corrective measure to prevent market failure.

The common remedies used to internalize various negative externalities are taxes and subsidies. However, the Internet challenges these definitions and the effectiveness of governmental measures on the issue of UCEs. The borderless nature of the Internet challenge the territorial rule and makes the definition of a relevant market to calculate externalities more difficult and

45. *Id.*
46. *Id.* at 80-81.

complicated. In the online market, externalities are cross-jurisdictional, meaning that the party causing an externality is often in a different country from the party paying for it. This makes the internalization of externalities very difficult due to various governmental authorities involved in attempting any enforcement. Take, for example, a situation where a spammer in China targets the US consumers through UCEs. The benefits earned by the Chinese spammers created great externalities on the US consumers and the national ISPs.[47] In such situation, it is nearly impossible for those affected by the externality to implement conventional measures such as taxes and subsidies to place the costs of UCEs back on spammers located in different jurisdictions. When externalities cannot be internalized, the market will likely head towards failure, which necessitates state intervention to prevent its failure. Therefore, by their very nature, UCEs' use of cross-border transactions necessitates multi-jurisdictional harmonization and state intervention to combat the negative effects of UCEs.

B. *Political Process*

As was previously discussed, market failure provides justification for state intervention. That said, the political process is not without its costs and should only be utilized when its benefits exceed the costs. The benefit of a regulation is the total increase of each participant's per capita stake.[48] The higher the per capita benefits are, the stronger an incentive for the participants to engage in the decision-making process. The costs associated with the political process are those of political participation, including the cost of collective group interests and the cost of preventing the free-rider problem.

In terms of business to consumer ("B2C") e-commerce, the benefits and costs of regulating e-commerce are uncertain and difficult to quantify, especially when e-commerce involves issues of globalization.[49] In terms of defining the benefits of regulating e-commerce, the advantages should be calculated based upon the entire participant base in the borderless e-market. As for the costs, e-commerce increases the complexity of calculating the costs of political participation, because e-commerce is founded upon cooperation between the international communities.[50] Thus, the rules and

47. According to the Spam Report conducted by Kaspersky Lab, China has been identified as the largest source of UCEs in the second quarter of 2013.
https://securelist.com/analysis/quarterly-spam-reports/37148/spam-in-q2-2013/ (last visited Sept. 14, 2015).

48. KOMESAR, *supra* note 33, at 68.

49. Larry E. Ribstein & Bruce H. Kobayshi, *State Regulation of Electronic Commerce*, 51 EMORY L.J. 1, 9 (2002).

50. Christopher T. Marsden, *Cyberlaw and International Political Economy: Towards Regulation*

structures of the political process such as jurisdiction, scope of legislation, etc., become more complicated, with higher costs that are difficult to predict.

The need for a legislative solution to the issues caused by UCEs is apparent given that more than seventy percent of the global e-mail traffic comprises UCEs, creating significant costs for consumers, corporations and ISPs. As was noted in the California Spam Legislation, California Business and Professions Code § 17529 (d), spam cost the United States organizations more than USD 10 billion in 2003 alone, including productivity and additional equipment, software, and manpower.[51] In 2012, the estimate for the cost of UCEs to consumers and corporations was between twenty and fifty billion dollars.[52] The estimate would be even more significant if calculated based on entire global market. The financial significance of these externalities necessitates legislation at the state level, along with efforts at the international level, in order to establish a standard of UCEs practices and decrease the harm caused by UCEs.

Most countries are developing spam regulations. In the United States, at the federal level, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" was enacted to combat UCEs. In addition, individual state level regulations have also been formulated. According to the statistics of the Nation Conference of State Legislatures as of 2010, there are thirty-seven states that have adopted anti-spam legislation.[53] In the European Union, an EU wide Directive was also announced to provide a basic standard to enact legislation to combat UCEs. Other countries, such as Japan, India, South Korea, Australia, Brazil and Canada are also enacting legislation to combat UCEs. Section III of this article will compare and discuss the legislative approaches adopted by the United States, European Union, and Japan to propose an encompassing solution for the regulation of UCEs.

C. *Adjudicative Process*

The adjudicative process as an institution has unique and significantly different characteristics from the market and political processes. Compared to the market, which is amorphous, the adjudicative process is more defined in terms of its jurisdiction and geographic boundaries. Contrasted with the political process, participants in the adjudicative process are far more

---

of the Global Information Society, 2001 L. REV. M.S.U.-D.C.L. 355, 363 (2001).

51. CAL. BUS. & PROF. CODE § 17529 (d) (2003).

52. Rao & Reiley, *supra* note 12, at 88.

53. STATE LAWS RELATING TO UNSOLICITED COMMERCIAL OR BULK E-MAIL (SPAM), NAT'L CONF. OF ST. LEGIS. http://www.ncsl.org/research/telecommunications-and-information-technology/state-spam-laws.aspx (last visited Sept. 14, 2015).

independent and fewer in numbers than those in the political process.

Generally, the adjudicative process has formal requirements for participation. Participants in the adjudicative process have to comply with these requirements and must bear the costs of accessing it. In addition, the adjudicative process is generally smaller in its scale, given that the participants are limited to specific issues. More importantly, in order to be effective, the adjudicative process needs to maintain its independence and fairness. However, maintaining independence and fairness in the adjudicative process comes at a significant cost.[54] These costs increase dramatically when cases involve international matters. Given that UCE issues generally involve cross-border activities, the evaluation of whether the adjudicative process is a proper institutional choice for regulating UCEs, requires a costs-benefit analysis.

Generally, the adjudicative process is passive, which means that the judge plays an essential role in the proceedings but does not actively initiate the adjudicative process. The complaining party initiates the process by filing a complaint containing causes of action based on legal arguments, giving rise to specific remedies including damages against the defendant. Based on the plaintiff's complaint, the Court adjudicates the issues presented.

The threshold access costs of initiating the proceedings become a significant determining factor for choosing the adjudicative process as an institutional choice. From filing a complaint to prosecuting a case, all the formalities and complexities of litigation require professional knowledge and experience. All costs associated with the litigation are shared by the disputing parties. These costs include researching and determining the merits of the complaint, investigating facts through the discovery process, representing and presenting the case to the court, and enforcing the final judgment.

Therefore, the cost-benefit test must focus on the parties to evaluate whether the benefits of utilizing the adjudicative process as an institutional choice will be higher than the costs of the damages done by UCEs. Naturally, if the benefits of obtaining a resolution through the adjudicative process are higher than the costs, the adjudicative process will be a preferable institutional choice, given its binding effects and enforceability.

1. *Costs of Resolving UCE Disputes through the Adjudicative Process*

Given the borderless nature of spam, factual discovery costs may become a major financial barrier. Most UCEs disguise their actual point of

54. KOMESAR, *supra* note 33, at 123.

origin. Tracking down the sender of UCEs is difficult, time-consuming and costly.[55] It also requires a high level of technical expertise.

For individual consumers, the technological barriers are too high and the stake per capita is too low to engage in the adjudicative process to resolve the UCE problem. A more affordable and practical choice for consumers is to seek out an ISP capable of providing a better spam filtering system or to simply ignore the annoyances caused by UCEs.

Comparatively, ISPs and corporations have more resources in terms of technology and capital. They also have a higher stake in resolving the burdens of externalized costs associated with UCEs. According to Ferris Research Inc., UCEs cost the United States organizations more than ten billion dollars in 2003.[56] In 2012, a conservative estimate concluded that spam related costs to American firms and consumers doubled to twenty billion dollars.[57]

Despite the high costs involved, litigation against spammers is still a very expensive option for corporations and ISPs, especially given that the enforcement of a judgment against a foreign spammer can be difficult and ineffective. The costs of locating spammers may not be an attractive investment when compared to the benefits derived from developing anti-spam technologies and enhancing technical infrastructure to handle UCEs.

The second significant costs of resolving UCEs through the adjudicative process are the costs of the litigation itself. Parties making a claim will have to absorb the costs of litigation itself. Litigation costs are generally the most crucial factor in the decision to choose the adjudicative process. The borderless nature of the Internet means that the UCE senders and receivers are often located in different countries, raising the prospect of cross-border litigation. According to the statistics conducted by Kaspersky Lab in August 2013, sixty percent of UCEs sent to European e-mail users originated in South Korea. Asia leads the world as a source of UCEs, followed by North America and Eastern Europe.[58] The statistics show that if consumers, corporations or ISPs were to adjudicate the legal issues concerning UCEs and sought damages against spammers through litigation, the litigation would likely involve international matters.

Cross-border litigation generally raises the entire cost of litigation. This is because cross-border litigation significantly increases information costs

---

55. CAL. BUS. & PROF. CODE § 17529 (i) & (j) (2003).

56. CAL. BUS. & PROF. CODE § 17529 (D) (2003).

57. Rao & Reiley, *supra* note 12, at 88.

58. TATYANA SHCHERBAKOVA & MARIA VERGELIS, SPAM IN AUGUST 2013, SECURELIST (Sept. 23, 2013, 03:05 AM), http://www.securelist.com/en/analysis/204792306/Spam_in_August_2013#7 (last visited Sept. 14, 2015).

due to the difficulties associated with conducting cross-border proceedings (e.g., language barriers, traveling costs, finding a competent foreign attorney, etc.). Furthermore, even if consumers, corporations or ISPs prevailed in a lawsuit, the enforcement of a judgment in a foreign country presents additional costs and uncertainties. Thus, the high costs associated with cross-border adjudication and a lack of international enforcement suggests that adjudicative process may not be an ideal institutional choice for combating spam.

2. *Benefits of the Adjudicative Process as an Institutional Choice*

Despite the high costs associated with the adjudicative process, the mechanism can still serve important functions in providing compensation for damages and allocating resources.[59] An effective and enforceable adjudicative process can also strengthen consumers' confidence in the Internet. Therefore, in order to maintain effectiveness of the adjudicative process in resolving UCE issues, decreasing litigation costs becomes crucial.

Decreasing ligation costs in cross-border legal disputes over UCEs requires strong cooperation between international communities in three regards. First, a unified standard for deciding jurisdiction should be established. Jurisdiction is a legal concept that determines where a lawsuit should be brought and tried. It goes without saying that the locality in which the lawsuit is tried has dramatic influence on the litigation costs. Second, alternative dispute resolution should be considered and developed to provide a more economical and time-saving process for resolving legal disputes involving UCEs. Arbitration also avoids the obstacles to bringing a lawsuit in a foreign country. Third, recognition and enforcement of an alternative dispute resolution judgment is crucial, given that unenforceability would render a judgment ineffective.

In summary, although the adjudicative process offers a number of advantages over the other institutional mechanisms, it can be costly for the participants. If the costs of seeking resolution through the adjudication process cannot be lower than the benefits to the parties who participate in the process, adjudicative process would not serve as a proper institutional choice for participants.[60] Effectively decreasing the costs associated with the adjudicative process is the key to strengthening the function of the adjudicative process in resolving various UCE issues.

---

59. KOMESAR, *supra* note 33, at 135.

60. Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915, 922 (2000).

III. REGIONAL EFFORTS IN COMBATING SPAM

Comparing the three primary institutional choices, the political process appears to be a more appropriate mechanism for regulating UCEs. The market appears to be an inefficient institutional choice given that the externalities created by UCEs reduce market participation and provide competition advantages to the UCEs senders by lowering transaction costs. Finally, market participants lack the incentive to engage in issues caused by UCEs. The adjudicative process is also limited in its ability to effectively resolve the issues posed by UCEs.

As the political process appears to be a more appropriate institutional choice for the regelation of UCEs, this paper compares different regulatory schemes, focusing on the United States, European Union and Japan with the goal of seeking an effective and practical international legal standard in regulating UCEs.

A. *The United States Model for the Regulation of UCEs*

1. *Threshold Challenges and the Constitutionality of UCE Regulation*

In the United States, the threshold challenges facing the regulation of UCEs are whether the states' anti-spam laws violate the dormant Commerce Clause of the US Constitution and whether regulating UCEs violates the First Amendment protection of commercial speech.[61] Regarding the first challenge, the validity of state anti-spam laws was decided by the Supreme Court of the State of Washington in the case of State v. Heckel. The Court held that the Commercial Electronic Mail Act, prohibits misrepresentation in the subject line or the transmission path of any commercial e-mail message sent to Washington residents or from a Washington computer, did not violate the dormant Commerce Clause since it does not unconstitutionally place a burden on interstate commerce. When an act does not facially discriminate against interstate and intrastate commerce and serves legitimate local interest of preventing cost-shifting from UCEs, the state has the inherent authority to regulate UCEs through the enactment of anti-spam laws.[62]

The second issue involves whether or not UCEs are protected commercial speech under the First Amendment and thereby exempt from regulation by the government. The US Supreme Court, in the case of Central Hudson Gas & Electric Corp. v. Public Services Commission, established a four-prong test for examining whether the government can lawfully regulate

61. State v. Heckel, 24 P.3d 404, 405 (Sup. Ct. WA. 2001).
62. *Id*. at 410.

commercial speech.[63] First, the commercial speech has to concern lawful activities and contain no misleading message in order to receive the protection of the First Amendment.[64] Second, if the commercial speech fails to meet the first test and falls within the purview of governmental regulation, the court will have to evaluate if the restriction on commercial speech can serve the substantial government interests asserted. Third, the court must determine if the regulation of commercial speech can directly advance the governmental interest asserted. Finally, the regulation must not be more extensive than necessary to serve the interest asserted. Examining these four criteria in dealing with the issue of UCEs, governmental regulation should be deemed constitutional if the following conditions are met:

(1) The purpose of UCE regulation is to establish a standard practice for regulating commercial e-mails and to prevent misleading or deceitful UCEs. As such, the benefits of UCEs can be promoted and utilized, with unjust cost-shifting externalities avoided or limited. One of the primary concerns with UCEs is that they generally contain misleading content in the body of the e-mail and in its subject line in order to trick the user into viewing the message.[65] In order to avoid being tracked, UCEs generally disguise their routing information and do not contain a return address. Moreover, some UCEs also misappropriate and unlawfully use registered trademarks in order to mislead the e-mail recipients as to the sponsorship and source of the product in order to gain more attention.[66] This type of unlawful UCE practice is not only deceptive but also constitutes trademark infringement. Therefore, the first criterion in regulating misleading or unlawful commercial speech is met when UCEs are involved.

(2) For the government to show a substantial interest in regulating commercial speech, the Supreme Court held in the case of Florida Bar v. Went For It, Inc., that the government does not need to produce empirical studies to show the significance of the harm it seeks to remedy.[67] Rather, the government can demonstrate the substantiality of its interest with anecdotes, history, consensus, and simple common sense.[68] Under this test,

63. Central Hudson Gas & Electronic Corp. v. Public Service Commission, 447 U.S. 557 (1980).
64. *Id*. at 564.
65. Scot M. Graydon, *Much Ado about Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L.J. 77, 107 (2000).
66. *LCGM, Inc*., 46 F. Supp. 2d at 448.
67. Florida Bar v. Went For It, Inc., 515 U.S. 618, 628 (1995).
68. *Id.*

the governmental interest in regulating spam is significant and apparent. The great externalities caused by UCEs through its inherent cost-shifting effects appeal to simple common sense. Receivers of UCEs, including individuals, corporations, and ISPs incur significant costs when exposed to spam. To ISPs, a great amount of investment is made in developing filtering systems designed to sort-out unwanted e-mails and reduce the impact of UCEs on the recipients.[69] The costs incurred by ISPs will be eventually shifted onto individuals and corporate Internet users. As discussed above, the estimated cost of spam to consumers and corporations in United States is over fifty billion dollars per year. Therefore, the government's interest in regulating UCEs is substantial. Even if only a fraction of the total cost of UCEs could be reduced, there would be a significant increase in the efficiency and usefulness of the Internet.

(3) Whether or not spam regulations can directly advance the governmental interest ought to be determined by looking at the specifics of each regulation. Analyzing the US spam rules at the federal and state levels, it is clear that the spam regulations generally focus on three dimensions: prohibition of fraudulent routing information, inclusion of a return address, and opt-out clauses for the recipients of UCEs.[70] These regulations focus on preventing misleading information and giving UCE recipients the control to decide whether they would like to receive the information sent to them.[71] These regulations accommodate the consumers' right to information by allowing them to decide when, what and how the commercial information will be received. Furthermore, they are able to ensure that the information is not fraudulent or misleading. Consequently, government interest can be directly advanced through establishing general practices for UCEs.

(4) The last test establishes whether the government's restrictions serving the interests claimed can be satisfied by showing that spam regulations are "narrowly drawn" to the governmental interest.[72] Even though direct marketers have the protection of

69. Controlling the Assault of Non-Solicited Pornography and Marketing Act § 2 (a)(3), 15 U.S.C. § 7701 (2003).

70. Graydon, *supra* note 65, at 108.

71. *Id.* at 109-10.

72. *See Public Service Commission*, 447 U.S. at 565.

> the First Amendment, this protection is not absolute.[73] Internet users also have rights to privacy and property. In order to balance these two interests, spam regulations can reasonably prohibit unlawful or misleading messages and balance the rights spammers and ordinary citizens. This, incidentally, also fosters the creation of criteria for good practices in direct marketing.[74] Given that more than seventy percent of e-mail traffic is composed of UCEs, any such regulation imposed must be necessary and narrowly tailored.[75]

2. *US Approaches for Regulating UCEs*

Recognizing the convenience and efficiency of electronic mail while acknowledging the abuse and damage caused by UCEs, the US Congress passed legislation entitled ''Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003'' ("CAN-SPAM Act"), which became effective in January of 2004.[76] The CAN-SPAM Act focuses on prohibiting false and misleading UCEs by requiring particular formalities for UCEs, identifying the enforcement authority, and imposing both civil and criminal liabilities on spammers.

(a) Requirements for Sending UCEs

(i) Prohibition of False and Misleading Transmission of UCEs

Pursuant to the policy of prohibiting false and misleading transmission of UCEs, the CAN-SPAM Act states that UCEs cannot contain any misleading or false information.[77] According to the Act, UCEs have to contain accurate header information, including the origin of the UCE, such as the e-mail address, the domain name and the Internet Protocol Address. Any pretense, disguise, or misrepresentation of the origin of the message in the e-mail address subject line or header information should be deemed as materially misleading and in violation of the Act.[78]

(ii) Prohibition of Deceptive Subject Headings

UCEs cannot contain a deceptive or misleading subject line that the senders knowingly utilize to mislead the recipients of UCEs.[79] This type of

---

73. *See e.g.*, Bread v. City of Alexandria, 341 U.S. 622, 642 (1951); Graydon, *supra* note 65, at 113.

74. Gary S. Moorefield, *SPAM —It's Not Just for Breakfast Anymore: Federal Legislation and the Flight to Free the Internet from Unsolicited Commercial E-Mail*, 5 B.U. J. SCI. TECH. L. 1, 10, 17 (1999).

75. Graydon, *supra* note 65, at 113.

76. 15 U.S.C. § 7701 (2003).

77. 15 U.S.C. § 7704 (a)(1)(A)-(C) (2003).

78. 15 U.S.C. § 7704 (a)(1)(B) (2003).

79. 15 U.S.C. § 7704 (a)(2) (2003).

misrepresentation is a violation of the unfair practice criterion under the Section Five of the Federal Trade Commission Act. Moreover, if a UCE contains sexually oriented material, it must provide a warning label in the subject line.[80] If the sender fails to include such a warning, he/she will be subjected to a fine under United State Code Title Eighteen, or imprisoned for no more than five years, or both.[81]

(iii) Inclusion of a Return Address and other Comparable Opt-Out Mechanism in UCEs for Recipients To Opt Out of Receiving UCEs

UCEs must include a valid return address or other comparable mechanisms, which allow the recipients to write back and express their unwillingness to receive any future communications.[82] The sender of UCEs is also required to maintain the capability to receive responses from the recipients and provide more details for the recipient to understand the mechanism to opt-out. If the recipient objects to receiving future transmissions, the sender must stop sending commercial messages within ten business days from the date of the receipt of the opt-out. Any messages sent after this time would constitute a violation of the Act.[83]

(iv). Clear and Conspicuous Notice of the Sender's Identification, Opt-Out Option and Physical Address

UCEs are required to clearly and conspicuously provide a notice of the sender's identification, opt-out options and valid physical address information.[84] The UCE sent should specify that the e-mail is an advertisement and a solicitation.[85] The e-mail must also provide a valid physical address of the sender, and an option to opt-out from future messages.[86] In addition, the Act authorizes the Federal Trade Commission ("FTC") to establish a national "do-not-e-mail" registry. This means that the UCE senders cannot send any unsolicited commercial electronic messages to the people who register on the list.

(b) Enforcement Authorities

The CAN-SPAM Act designates the FTC as the federal enforcement authority. It provides the grounds for civil action against spammers by either state attorney generals or ISPs.[87] Given that the nature of combating spam generally requires international cooperation, the US Congress enacted the "Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders Act of 2006" (SAFE WEB Act), allowing the FTC to police

80. 15 U.S.C. § 7704 (d)(1) (2003).
81. 15 U.S.C. § 7704 (d)(5) (2003).
82. 15 U.S.C. § 7704 (a)(3) (2003).
83. 15 U.S.C. § 7704 (a)(4) (2003).
84. 15 U.S.C. § 7704 (a)(5) (2003).
85. 15 U.S.C. § 7704 (a)(5(i) (2003).
86. 15 U.S.C. § 7704 (a)(5)(i)-(iii) (2003).
87. 15 U.S.C. § 7706 (a), (f), (g) (2003).

illegal spam, spyware, cross-border fraud and deception.[88] The SAFE WEB Act extends the FTC's power to cross-border investigations against spammers. According to the Act, the FTC can share information with foreign enforcement authorities. In the first report to the Congress in 2007, the FTC applied the Act to share its information with the Australian and Canadian enforcement authorities to stop spammers.[89] The SAFE WEB Act enhanced the FTC's functions in combating UCEs and was well received. It however contained a sunset provision, specifying that the Act shall cease to have effect seven years after its enactment, which was in 2013.[90] Given that the Act provided the FTC with an effective tool to combat online fraudulent activities, Congress extended the Act to September 30, 2020.[91]

(c) Criminal and Civil Liabilities Imposed on the Senders of Unlawful UCEs

CAN-SPAM Act imposes both criminal and civil liabilities on the senders of unlawful UCEs. The Act amended Chapter Forty-Seven of Title Eighteen, United States Code by adding Section § 1037, "Fraud and Related Activity in Connection with Electronic Mail."[92] The Act establishes a fine and criminal penalty for violations. If the senders violate the Act, they will be fined, imprisoned for up to five years, or both.[93]

The Act also provides for statutory damages. When a state brings action against a spammer, the statutory damages are calculated by multiplying the number of violating UCEs by damages of up to two hundred and fifty dollars ($250) per UCE, based on the type of violation.[94] The total amount determined cannot exceed two million dollars (USD 2,000,000).[95] However, if a court finds that the defendants knowingly and willfully violated the Act, the court can increase the final award by up to three times the amount of the statutory damages.[96] In the event of any successful action, the court has discretion to grant the cost of the action and reasonable attorneys' fees to the state.[97] If the action is brought by a Provider or Internet Access Service, the statutory damages are calculated up to one hundred dollars ($100) per e-mail

88. Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2006 § 4, 15 U.S.C. 46 (2006).

89. FEDERAL TRADE COMMISSION, THE U.S. SAFE WEB ACT, THE FIRST THREE YEAR, REPORT TO CONGRESS (2009), https://www.ftc.gov/sites/default/files/documents/reports/u.s.safe-web-act-first-three-years-federal-trade-commission-report-congress/p035303safewebact2009.pdf.

90. *See*, *e.g.*, 15 U.S.C. 46 § 7 (2006); Mutchler, *supra* note 25, at 965.

91. H.R. 6131, 112th Cong. (2012) (the bill was later signed into a law by US President Obama).

92. *See, e.g.*, 15 U.S.C. § 7703; 18 U.S.C. § 1037.

93. *Id.* (whether spam should be criminalized is still arguable. This provision, however, shows Congress' determination to combat spam).

94. 15 U.S.C. § 7706 (g)(3)(A) (2003).

95. 15 U.S.C. § 7706 (g)(3)(B) (2003).

96. 15 U.S.C. § 7706 (g)(3)(C) (2003).

97. 15 U.S.C. § 7706 (g)(4) (2003).

violation and the maximum award cannot exceed one million dollars per violation.[98]

Analysis of the Act suggests that it is frequently invoked against spammers. In recent years, more and more spammers were prosecuted or sued for their violation of the CAN-SPAM Act and other state level anti-spam legislations. These actions were brought both, from the State sector such as the FTC and also from the private sector by companies such as My Space and Facebook, Inc. One of the most significant damages awards was granted by the District Court of Northern California in the case of Facebook, Inc. v. Sanford Wallace, et al.[99] The court granted the statutory award in the amount of $711,237,650 for defendant's violations under the CAN-SPAM Act and the California Business & Profession Code § 22948.2. The defendant, Sanford Wallace was also later prosecuted by the U.S. Attorney's Office and found guilty by a federal grand jury on multiple counts of fraud. Despite the low possibility of collecting the entire award, state and private service providers expect that the outcome of these civil and criminal trials will create a deterrence effect on spammers.

However, not every lawsuit against UCEs senders were successful. In recent cases, Rosolowski v. Guthy-Renker LLC and Rosolowski v. People Media, Inc., the California Court of Appeal ruled in favor of UCE senders.[100] In these two cases, consumers claimed that both Guthy-Renker LLC and People Media, Inc. misleadingly listed unregistered and fictitious sender names. Furthermore, the e-mail subject lines of the messages contained misleading information. As such, the consumers claimed that the senders violated California's Restrictions on Unsolicited Commercial E-mail Advertiser Law § 17529.5(a)(2) and (a)(3). The Court affirmed the trial court's decision and held that even though the senders' identity cannot be identified from the e-mail address line, no violation occur as long as it is evident from the content of the e-mail that the sender's identify can be ascertained.

The same logic was applied to the issue of misleading e-mail subject lines. According to the Court of Appeals, as long as the content of the e-mail provides conditions of the claims or offers made, the subject line is not misleading.[101] The practical implication of this decision is that it is permissible for UCE senders to use different domain names that have no connection to their official names with misleading language in subject line of

98. 15 U.S.C. § 7706 (g)(3)(A)(i) (2003); 15 U.S.C. § 7706 (g)(3)(B) (2003).

99. Facebook, Inc. v. Wallace, No. C 09-798 JF (RS), 2009 WL 3617789 (N.D.Cal. Oct. 29, 2009). Case not reported in F. Supp. 2d.

100. Rosolowski v. Guthy-Renker LLC, No. B250951 (Cal. Ct. App. Oct. 29, 2014); Rosolowski v. People Media, Inc., No. B250482, 2014 WL 5472450 (Cal. Ct. App. Oct. 29, 2014).

101. Evan Brown, *Internet Law Regulatory and Litigation Matters*, 18 J. INTERNET L. 30, 33-34 (2015).

e-mails as long as this information can be clarified from the content of the UCE. These decisions, therefore, limits the practical application and enforcement of anti-spam laws.

B. *The European Union Model for the Regulation of UCEs*

1. *European Union's Developments in UCE Regulation*

The EU has long recognized the problems associated with UCEs and has launched campaigns to strengthen the Internet users' and businesses' awareness of issues related to spam. The European Parliament and the EU Council announced the Data Protection Directive in 1995 in order to ensure the protection of individuals regarding the processing of personal data and the Free Movement of Such Data.[102] The motivating factor behind the passage of this directive was the concern over the protection of privacy. When a message contains personal information and is transmitted via electronic mail, the necessity of standardized procedures for handling personal data is crucial to maintaining the free flow of information and safeguarding personal rights to privacy.

In order to address the goals identified in the Data Protection Directive, the European Parliament and the Council subsequently enacted the E-Commerce Directive on June 8th, 2000. The Directive seeks to harmonize legal aspects of information society services[103] and, in particular, the e-commerce in the EU.[104] The Directive notes that UCEs are undesirable as they disrupt the smooth functioning of interactive networks and place additional communication costs on the recipients. In addition, the Directive also promotes transparency on various UCE related regulations and facilitation of the function of such industry initiatives. Article Seven of the Directive establishes basic requirements for the member states to follow when enacting domestic UCE regulations.[105]

The most recent directive that focuses on UCEs is the EU Directive on Privacy and Electronic Communications, passed in 2002.[106] The Directive continues to emphasize a right to privacy and intends to provide safeguards

---

102. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

103. The Directive defines "Information Society Services" as activities of an interactive nature provided online with economic value.

104. Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1 [hereinafter Directive on E-Commerce].

105. Directive on E-Commerce art. 7.

106. Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 on Privacy and Electronic Communications, 2002 O.J. (L 201) 37 [hereinafter Directive on Privacy].

against UCEs' intrusion on personal privacy. It further encourages member states to establish a harmonized standard to ensure simple, EU community-wide rules for businesses and users as to balance the interest of direct marketing with personal privacy protections. Furthermore, this Directive required all member states to implement the provisions necessary to comply with this Directive by October 31, 2003.[107]

However, few member states met this deadline and failed to enact anti-spam laws. In 2004, the EU instituted proceedings against the countries that did not comply with their obligations under the Directive. By 2007, all member states finally enacted the necessary legislation in accordance with the Directive.[108]

2. *European Union's Approaches to Regulating UCEs*

As was articulated in various EU Directives, the goals of regulating UCEs is to create the appropriate privacy protections, ensure smooth functioning of the Internet, and establish a unified standard of rules for regulating the direct marketing industry. The three Directives described above expect that regulating UCEs to balance the convenience and effectiveness of e-mail and also protection to users' right to privacy and information. The mechanism established by the Directive on E-Commerce and later supplemented by Directive on Privacy shows the evolving EU policies on UCEs.

(a) Mechanism Established Under the Directive on E-Commerce

Article Seven of the Directive on E-Commerce established two requirements for UCEs. First, it requires the UCEs to provide clear and unambiguous identification information.[109] Member States' domestic laws are required to ensure UCEs communicated by service provider should be clearly identified as an unsolicited commercial message.[110] Second, the Directive also requires member states to take measures to establish an opt-out registry, which allows individuals to register and opt out the list of UCEs receivers. The Directive requires the member states to impose the regulation requiring service providers to review the list regularly and respect the opt-out choices by the registers in order to ensure that any UCEs sent are not directed to any email registered with the list.[111] All member states were required to comply with this rule and had to pass domestic legislation by

107. Directive on Privacy art. 17.

108. Mutchler, *supra* note 25, at 973-74.

109. Member States' domestic laws are required to ensure UCEs communicated by service provider should be clearly identified as an unsolicited commercial message. Directive on E-Commerce art. 7(1).

110. Directive on E-Commerce art. 7(1).

111. Directive on E-Commerce art. 7(2).

January 17th of 2002.

Although ambitious, the mechanism under the Directive on E-Commerce did not appear to be effective. While opt-out registries appeared to be a sound policy to regulating spam, the list of valid e-mail addresses itself became the target of spammers. For spammers, the registry became a valuable database that decreased their costs associated with obtaining valid e-mail accounts.[112] Furthermore, enforcement of the registry system at the state level was also problematic. Without other methods of enforcement, states policed UCES by imposing a vague duty on service providers to regularly check the registry. This system did not appear to be effective in preventing spammers from sending UCEs.[113]

(b) Current Mechanism Established by the Directive on Privacy

Article Thirteen of the Directive on Privacy adopts a different approach to regulating UCEs. Instead of the opt-out mechanism adopted by the Directive on E-Commerce, the Directive on Privacy adopts an opt-in mechanism. The opt-in mechanism means that any direct marketing communication cannot be sent to any e-mail account without the account holder's consent.[114] Even after obtaining the explicit consent, UCE senders must provide the recipient with an easy means of objecting to future transmissions.[115] If the transmission of email is not for the purpose of direct marketing, the member states also have to adopt a measure to prohibit transmissions that were sent without subscribers' consent.

In addition, the Directive on Privacy also requires UCE senders to provide their identities with a valid address where they can be reached by the recipients notifying them of their desire to stop receiving future communications.[116] Any disguise of the sender's identity is prohibited by the Directive.

The Directive made an interesting distinction between natural and legal persons. It adopted the opt-in requirement for natural persons. However, for legal persons, such as a corporation, the Directive leaves the issues to member states to enact laws to adopt the mechanism that can also sufficiently protect that legal person.[117]

(c) Difficulties Associated with EU Directives

Although the EU Directives recognize the importance of consistent and harmonized standards for regulating UCEs, the EU Directives are facing two significant challenges in terms of effectiveness of those provisions. The first

112. John Magee, *The Law Regulating Unsolicited Commercial E-mail: An International Perspectives*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 367 (2003).

113. Mutchler, *supra* note 25, at 971.

114. Directive on Privacy art. 13 (1).

115. Directive on Privacy art. 13 (2).

116. Directive on Privacy art. 13 (4).

117. Directive on Privacy art. 13 (5).

challenge is the enforceability of the rules outlined in the Directives at the national level. Even though the EU adopted stricter regulations than the U.S., initially, only eight countries adopted the opt-in mechanism in their domestic anti-spam laws.[118] This non-compliance forced the Commission to put formal pressure on member states in the form of requesting their reasoning for failing to comply. The lack of enforceability was further demonstrated when the Commission brought legal action against France, Luxembourg, Netherlands, Germany and Ireland before the European Court of Justice for non-implementation of EU Community obligations.[119] Finally, by 2007, most of the member states had enacted the anti-spam legislation required by the Directive on Privacy.

The EU Directives also fail to effectively target spammers due to the lack of harmonization and consistent enforcement at the domestic level.[120] Even though the principles are enacted by the Directives, interpretation and implementation is left to each member state. Specifically, each member state enacts domestic legislation according to its interpretation of the ambiguous provisions outlined in the Directives. This lack of harmonization can cause difficulties for the free movement of personal data and threatens the effectiveness of the Directives. The EU Commission also recognized the necessity to promptly address these challenges. In its 2006 report 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, addressed the necessity of increasing legal enforcement to combat spam through international cooperation.[121]

C. *The Japanese Model for the Regulation of UCEs*

In the Asia region, since 2002 Japan enacted the Anti-Spam Law to combat UCEs and proposed several amendments ever since. Originally, UCEs in Japan were sent primarily to mobile devices, but more recently, UCEs are sent to personal computers.[122] A survey was conducted in 2004 and 2006 regarding the target device in Japan. In 2004, 73% of UCEs were sent to mobile devices and only 27% were sent to PCs. However in 2006, only 13% of the UCEs were sent to mobile devices and 87% were sent to

118. These countries are: Austria, Belgium, Denmark, Finland, Germany, Greece, Italy, and Spain, http://www.euro.cauce.org/en/countries/index.html.

119. Andrew Charlesworth, *Information Privacy Law in the European Union*, 54 HASTINGS L.J. 931, 937 (2003).

120. *Id.*

121. Mutchler, *supra* note 25, at 974.

122. A survey was conducted in 2004 and 2006 regarding the target device in Japan. In 2004, 73% of UCEs were sent to mobile devices and only 27% were sent to PCs. However in 2006, only 13% of the UCEs were sent to mobile devices and 87% were sent to PCs.

PCs. The dramatic shift in this trend called for the need to amend Japan's anti-spam regulations.[123] In 2002, Japan first enacted two anti-spam laws entitled the Act on Regulation of the Transmission of Specified Electronic Mail and the Act for Partial Amendment to the Law on Specified Commercial Transactions Law.[124] In 2005 and 2008, the law on Regulation of the Transmission of Specified Electronic Mail was amended to combat the new developments in UCEs.[125]

Generally speaking, Japan's law combines the virtues of both US and EU's approaches to regulating UCEs. The scope of UCEs regulated includes all commercial e-mails sent by organization for profit and a person in cases where the person is engaged in business to or from Japan to other persons as a means of advertisement for sales activities.[126] The definition of UCEs under Japan's anti-spam law is relatively broad. As such, it covers a wide range of UCEs. It provides guidelines and standards for regular and legitimate direct marketing e-mails and empowers authorities to impose liability on spammers.[127] Japan's 2008 revised anti-spam law has four main pillars. These aspects of the regulatory system are discussed below:

1. *Opt-In Mechanism*

Japan new anti-spam law adopts the EU approach and switches its approach from an "opt-out" to "opt-in" which forbids UCEs senders from distributing any UCEs unless it has the recipient's consent.[128] The opt-in approach is used because the opt-out system, such as the one used by the United States, is seen to be insufficient to block out unwanted UCEs. By imposing the requirement of obtaining consent before sending UCEs information autonomy back can be switched back to recipients (i.e. primarily general consumers) and effectively filter out unwanted UCEs.[129] Pursuant to

123. HIROYO HIRAMATSU, JAPAN'S COUNTERMEASURES AGAINST SPAM, MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS, JAPAN (2007), http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/070410_2.pdf.

124. DENNIS DAYMAN, ISSAC RASKIN YOUNG & CHARLES A. KARWOWSKI-HOPPEL, JAPAN NEW ANTI-SPAM LAW (Jul. 29, 2008), http://www.mofo.com/news/updates/bulletins/14219.html.

125. Overview of Japan Anti-Spam Law, MINISTRY OF INTERNAL AFF. AND COMM. IN JAPAN, http://measures.antispam.go.jp/pdf/overview%20of%20Japanese%20anti-spam%20law.pdf.

126. Tokutei Denshi Mēru no Sōshin no Tekisei-ka-tō ni Kansuru Hōritsu [Act on Regulations of the Transmission of Specified Electronic Mail] (2009), art. 2 paras. 1, 2 (Japan) (i), (ii). (2009) [hereinafter Japan Anti-Spam Law], http://measures.antispam.go.jp/pdf/Japanese%20anti-spam%20law.pdf.

127. Japan's new anti-spam law has five chapters. Chapter One regulates general provisions. Chapter Two focuses on measures for the appropriate transmission of specified electronic mail and provides guidelines of transmitting UCEs. Chapter Three stipulates registered agency for proper transmission. Chapter Four lists miscellaneous provisions. Chapter Five imposes penal provisions for the violations of the anti-spam law. *See id*.

128. Japan Anti-Spam Law art. 3.

129. *See* YOUNG & KARWOWSKI-HOPPEL, *supra* note 124, at 2.

Article Three of the new anti-spam law, the senders of UCEs can only send UCEs under the following criteria: a) the recipient grants his/her consent to receive UCEs prior the transmission; b) the recipient has provided the sender with his/her e-mail address specified in the applicable ordinance; c) the recipient has a business relationship with the sender and uses e-mail as a means to advertise related sales activities; d) the individual recipient or the organization publicize their own e-mails.[130] The senders are also required to maintain records that prove that they obtained recipients' consent prior the transmission of UCEs.[131]

2. *Labeling Requirement and Prevention of Fictitious and False Information*

According to the law, the UCE senders are required to accurately and clearly disclose their information and label their messages with relevant identifying information. Japan's Ministry of Internal Affairs and Communications enacted the Ordinance for Enforcement of the Act on Regulation of the Transmission of Specified Electronic Mail, stipulating the labeling requirements.[132] Pursuant to Articles Four to Six of the Anti-Spam Law, the senders of UCEs are prohibited from transmitting false information or using fictitious e-mail addresses to disguise their identities in their sales activities.[133] Where a violation of these rules occurs, the Minister of Internal Affairs ("MIC") may issue administrative orders requiring the senders to take necessary measures needed for compliance. Since the amended law entered into force in 2008, the MIC has issued more than 20 administrative orders to request UCEs senders to comply with the opt-in requirement and also to punish the sending the email with false sender information.[134]

3. *Creation of a Communication Agency*

One of the unique approaches of Japan's New Anti-Spam law is a requirement to set up an agency to coordinate communications between individuals and authorities. In order to enhance the implementation and enforcement, the anti-spam law grants the MIC minister authority to allow

130. Japan Anti-Spam Law art. 3, paras. 1-5.

131. Japan Anti-Spam Law art. 3, para. 2.

132. Tokutei Denshi Mēru no Sōshin no Tekisei-ka-tō ni Kansuru Hōritsu Shikōkisoku [Ordinance for Enforcement of the Act on Regulation of the Transmission of Specified Electronic Mail], Act No. 26 of 2002 (Japan), http://measures.antispam.go.jp/pdf/Ordinance%20for%20Enforcement%20of%20the%20Act%20on%20Regulation%20of%20the%20Transmission%20of%20Specified%20Electronic%20Mail.pdf.

133. Japan Anti-Spam Law art. 4-6.

134. *See* MINISTRY OF INTERNAL AFF. AND COMM. IN JAPAN, *supra* note 125, at 4.

the registration of an agency for the proper transmission of communications. The agency primarily provides services to assist any person who intends to file a petition to the MIC concerning suspected violations of the anti-spam laws. Furthermore, the agency conducts investigations concerning the alleged violations and provides the MIC with information and materials related to the suspected violation.[135] By cooperating with the MIC's efforts, a registered agency can provide a wider range of monitoring and enforcement services in the area of anti-spam law and activities.

The registered agency created for the proper transmission was the Japan Data Communications Association (JADAC).[136] JADAC established the Anti-Spam Consultation Center ("ASCC") in July 2002. The ASCC typically divides its anti-spam activities in four stages. In the first stage, individuals or corporations receiving unwanted UCEs notify the ASCC. After the ASCC received the compliant, it analyzes the legality of the claim. Typically, the ASCC examines whether the UCEs sent are in violation of the new anti-spam law such as failing to comply with labeling requirements, sending the UCEs to the person without obtaining prior consent, disguising or falsifying senders' information. Once the ASCC finds that the UCEs do indeed violate relevant anti-spam laws, the ASCC reports its investigation to the MIC. The MIC is then able to take legal action against the sender.

Through this cooperation with the private sector, Japan has extended and widened its efforts in combating spam. Overall, the policy appears to be effective in deterring spam activities. According to the Kaspersky Laboratories report on spam and phishing activities, in the first quarter of 2014, spam and phishing activities in Japan only represented only 1.92 percent of total spam activities worldwide. Comparatively, the rate is 18.81 percent in the United States.[137]

4. *Criminal Penalties*

Japan also adopts the US approach of imposing criminal penalties on the sender who is in the violation of anti-spam law. The highest criminal penalty for a violation is up to one year imprisonment and the fine up to one million yen.[138] Compared to the US CAN-SPAM Act, the criminal penalties

135. Japan Anti-Spam Law art. 14.

136. The Japan Data Communications Association (JADAC), was established to promote Japanese information communication technology industry in December 1973. JADAC established the Anti-Spam Consultation Center (ASCC) in July 2002 and has become a designated registered corporation under the Japan new anti-spam law.

137. Spam and Phishing Statistics Report Q1-2014, KASPERSKY LAB, http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014#.VTkFCGSeAXB (last visited Sept. 23, 2015).

138. Japan Anti-Spam Law § 33-38.

stipulated under Japan's anti-spam law are lighter. In addition, the criminal penalties focus more on the violation of the administrative order or the failure to comply with record keeping and labeling requirements. On the civil liability side, Japan does not provide for statutory damages as is done by the US.

IV. PROPOSALS AND CONCLUSIONS

The purpose of this article is to propose a regulatory solution that can exploit the benefits of UCEs and limit the externalities associated with them. As was discussed throughout this article, the conveniences and effectiveness of UCEs make it an economical and efficient direct marketing tool. They significantly decrease transaction costs and increase the competitiveness of markets. Nevertheless, due to their inherent nature of cost-shifting effects, UCE senders bear only nominal costs in sending out enormous numbers of UCEs and impose externalities on Internet users and ISPs. More importantly, many UCEs contain deceptive and misleading messages, and are, at times, loaded with malware designed to harm the recipients. Given that UCEs make up more than seventy percent of the global e-mail traffic, a proper institutional choice is needed to find a balance between the benefits of UCEs and their costs.

After analyzing the three primary institutional choices, the market, the political process and the adjudicative process, the real potential for market failure and ineffectiveness of adjudicative process in addressing the UCE issue lead to the conclusion that the political process is a more appropriate institutional choice for regulating UCEs. Furthermore, analysis of the regulatory systems in the United States, the European Union and Japan, leads to the conclusion that the borderless nature of UCEs creates legal issues that require international cooperation and harmonization of legal standards to to be implemented into their regulatory schemes in order to effectively resolve UCEs issues and strengthen global enforcement.[139]

Therefore, this article proposes several suggestions in order to establish a framework for regional and national legislation and to foster a global legal standard for regulating UCEs. Regulating UCEs by legislation can increase the combined interest of the majority and establish "good practice" standards for the direct marketing industry. The goal is that by setting practical standards for transmitting UCEs, the benefits of UCEs can be reaped from commercial transactions and the externalities caused by costs shifting effect can be limited. This will ultimately foster a sound and sustainable

139. FEDERAL TRADE COMMISSION, *supra* note 89. FTC's report to US Congress and European Council's Communication to the Parliament recognize the importance of international cooperation and enforcement.

commercial environment for electronic transactions and contribute to maintaining the free flow of information.

A. *Transparent UCEs Practice Standards*

In order to establish a "good practices" standard for UCEs in the direct marketing industry and protect consumers' right to information and privacy, a transparent UCEs practice standard is necessary. The purpose of such standard is to highlight the commercial utility of UCEs while eliminating misleading and deceptive messages. One crucial aspect of such standard would be a requirement to clearly and unambiguously identify the UCEs as advertisements that contain no misleading or deceptive information. Therefore, several key elements of UCEs must be addressed on to establish standards for transparent UCEs practice.

1. *Subject Line Labeling Requirements*

UCE senders should identify their messages as commercial advertisement in the subject line of the e-mail. A clearly labeled subject line can allow the account holders to appreciate the nature of the e-mail received. Furthermore, these labeling requirements will also improve the effectiveness of UCE filtering software. Receivers, including individuals, corporations and ISPs, will be able to identify UCEs and screen out any unwanted messages.[140]

This solution is not without its shortcomings. Specifically, spammer compliance becomes a major problem when considering the effectiveness of this requirement. It is reasonable to assume that most illegal spammers will never comply with these labeling requirements and only legitimate UCEs will be blocked by the filtering software.[141] Nevertheless, this requirement is still useful when combined with an opt-in system (discussed below). As consumers opt in to receive UCE messages, the labeling requirements will allow them to clearly identify the nature of the e-mails. Moreover, the purpose of establishing a good standard for UCE practice is also beneficial for the market as a whole.

2. *Clear and Complete Sender Information*

UCE senders should provide clear and complete information regarding the sender's identity, in order to meet the requirement of transparency. The

140. FEDERAL TRADE COMMISSION, SUBJECT LINE LABELING AS A WEAPON AGAINST SPAM (2005), http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf.

141. *Id*. at 6.

minimum requirements of sender information should provide the UCEs receivers with sufficient information to identify and contact the sender. The identifying information should, at the very least, include the sender's name, who the message is being sent on behalf of, electronic and physical return address, correct routing information, and contact information.

3. *No False or Misleading Information*

In order to protect consumers' rights to information, UCEs should not contain misleading or deceptive information. This requirement is aimed at removing the common practice of UCEs misappropriating third parties' trademarks with the goal of causing confusion in the receiver as to the sponsorship of the UCE for malicious purposes such as attracting click through traffic. This "free-rider" practice is damaging to the market and must be prohibited.

B. *Decreasing the Externalities Caused by the Costs-Shifting Effect*

The costs-shifting effect of UCEs allows spammers to exploit the benefits of spam by imposing externalities on the recipients. This results in an unjust allocation of resources since the person benefiting from the transaction does so at the expense of others. In order to resolve this issue, any legislation proposed should focus on decreasing the externalities and transferring UCE related costs back onto the senders. Therefore, the following measures should be considered for regulating UCEs.

1. *Opt-In Mechanism*

The US and the EU have adopted different means for consumer control of UCEs. The US mainly adopts the opt-out approach;[142] the EU Directive on Privacy adopts the opt-in approach.[143] The primary difference between these two approaches is that in the opt-in mechanism, the receiver is actively granting his or her consent to receive UCEs. In contrast, in the opt-out mechanism, the receiver is passively declining to receive UCEs. Comparing these two mechanisms, the opt-in mechanism appears to be more effective in decreasing spam and reducing the externalities imposed on the receivers.

The opt-in mechanism requires the UCE senders to obtain the UCE receiver's consent before sending commercial messages. The sender, therefore, has to bear the costs of providing an opt-in option, including the

142. 15 U.S.C. § 7704 (a)(5) (2003).
143. EU Directive on Privacy in E-Communications ¶45.

costs associated with obtaining consent, confirmation and disclosure of the opt-in mechanism. The costs of providing opt-in mechanism can be varied based on the legislation, such as in cases where electronic signatures can be utilized to obtain consent.[144] The costs of obtaining consent balance the costs-shifting to the receiver and allow the receivers to control the access to information. Granting consent also justify the costs and consideration on the receiver side to access information. In addition to the opt-in option, after the UCEs sender obtains consent from the receiver, the sender should also provide a clear and easy mechanism for the receiver to withdraw his consent.

From the viewpoint of consumer protection, the opt-in option is the most effective mechanism for regulating spam. By implementing an opt-in system, consumers can actively control access to their e-mail addresses by giving consent before spammers can send out UCEs. If consumers are passively given an option to opt-out through a registration list, they have to bear the risks and burdens of receiving the UCEs before they opt-out. Under this model, externalities caused by the cost-shifting effects of UCEs cannot be limited. Moreover, in the situation where consumers do not have sufficient knowledge of how to exercise their rights to opt-out, the mechanism will fail to deter UCEs.

In summary, in order to protect consumer rights and prevent spammers from taking advantage of consumers on the account of their insufficient knowledge of the opt-out process, the opt-in option should be considered as a better solution. In addition, by adopting the opt-in mechanism, the UCE senders will more likely meet the transparency requirements by properly formatting UCEs in order to gain consumers' trust.

2. *Remedies and Enforcement*

The EU Directive on Privacy did not establish a standard remedy and left it to the member states to enact through their local laws. In much the same way, each state in the US has different standards regarding remedies for spam violations.

Establishing a remedy standard is important for two reasons. First, a clear remedy standard can provide legal certainty for consumers and ISPs in estimating the losses and benefits associated with legal action. It also directly relates to spammers' calculations for risk control. Second, a consistent standard for remedies can prevent spammers from forum shopping in order to take advantage of differences in remedy standards between various jurisdictions.

Nevertheless, any remedy standard will be meaningless if it lacks an

144. Ribstein & Kobayashi, *supra* note 49, at 27.

effective mechanism for enforcement. If any legal decision or a penalty cannot be eventually enforced, the effectiveness of UCE regulations will be undermined. As more anti-spam cases are prosecuted in American courts and substantial damage awards are granted, if these judgments cannot be enforced, such awards will have only a nominal meaning and be without any effect.

Due to the borderless nature of UCEs, international cooperation in enforcement is particularly important. In order to avail themselves from regulation and legal action, spammers generally target e-mail recipients located in different jurisdictions. This increases the difficulties associated with investigation, prosecution and enforcement. Given that technology facilitates fraudulent and deceptive commercial activities across national borders, the difficulties in combating these activities necessitate international cooperation and enforcement mechanism. The Organization for Economic Cooperation and Development ("OECD") "Guideline for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders" provides great insights and key elements for such international corporation to become effective.[145]

The establishment of an effective cross-border enforcement mechanism requires several key factors. The first factor is information sharing and investigation cooperation. Given that the Internet and new telecommunication technologies provide great ease for spammers to send UCEs in different territories easily, states need to foster judicial cooperation in terms of sharing investigation information and establishing notification channels.[146] As such, any authorities in the incident related countries would be able to obtain sufficient information and evidence to take timely action. The US Safe Web Program provides a great example of cross-border information sharing. By establishing a network for monitoring and sharing spam relevant information among national authorities, the initiative significantly increased the effectiveness of global investigations, prosecution and enforcement.

A second key factor in establishing an effective cross-border mechanism for regulating UCEs is to maintain an effective domestic system to combat

---

145. The Organization for Economic Co-Operation and Development (OECD) was established on September 30th, 1961 pursuant to the Paris Convention signed on December 14th, 1960. The founding member countries are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The goal of OECD is to achieve highest sustainability and economic growth in member countries and contribute to the global economic growth. At the time of writing, thirty-four countries are member of the OECD. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDELINES FOR PROTECTING CONSUMERS FROM FRAUDULENT AND DECEPTIVE COMMERCIAL PRACTICES ACROSS BORDERS (2003), http://www.oecd.org/sti/ieconomy/37125909.pdf [hereinafter the Guideline for Consumer Protection].

146. *Id.* at 10.

fraudulent activities. In order for the international cooperation to be effective, each country should maintain effective legal and administrative measures. Each domestic mechanism can then be extended and strengthen by connecting with other domestic systems as to form a comprehensive international framework to combat UCEs.[147]

The third key factor is broad cooperation with the private sector, including various ISPs, domain names registry providers, individual consumers and consumers groups, financial institutions and corporations. Investigation, prosecution or enforcement of UCE laws requires private sectors' supports and continuous inputs to be effective. The private sector can take initiatives and also provide substantial supports to governments, including filing complaints, providing information, establishing self-regulation, initiating litigation and participating in enforcement. One successful example of cooperation with the private sector's self-regulation and governmental efforts has been shown in Japan's combat against mobile spam by mobile carriers along with government authorities. By working with the government, once the government confirmed the sender of mobile spam, mobile carriers would suspend the account used to send out UCEs. The number of UCEs sent to mobile devices markedly decreased from 2003 to 2005 since the mobile carrier joined the efforts.[148] During these three years, the numbers of UCEs sent to mobile devices dropped to almost zero. Supported by such encouraging results, ISP possesses the ability to control and monitor the senders of UCEs. By cooperating with government authorities to report, monitoring, supporting and eventually suspending the service by terminating the service contract, private and government sector cooperation can provide great enforcement abilities to the combat UCEs.

3. *Accountability of ISPs*

Generally speaking, ISPs are most likely to be viewed as victims of the senders of UCEs, however, it is the ISPs themselves that actually facilitate the dissemination of UCEs.[149] If legislation holds ISPs accountable to other ISP's losses resulting from UCEs transmitted through an ISP's network, the benefit of providing Internet services could be significantly less than the costs and risks of damages. By holding ISPs accountable, the UCE issue could be nipped in the bud by encouraging ISPs to limit spammers' access to potential victims. The basic norm of holding ISPs accountable is that an ISP

147. *Id.* at 11.

148. *See* HIRAMATSU, *supra* note 123, at 12. The number of the UCEs sent to mobile devices dropped significantly from 2003 to almost zero in 2005, since the private sector enforces government's spam policy.

149. *See* Soma, Singer & Hurd, *supra* note 2, 186-93.

also gains benefits from spamming.

Furthermore, technically speaking an ISP has a better ability to control what it transmits when compared to private individuals. Some ISPs have implemented validation programs, which limit the transmission of e-mails that do not comply with certain format requirements. For example, Comcast, a US ISP, has implemented a webmail system that uses only ".csv" file types, banning e-mails that are not configured to Comcast's requirements.[150] With the transmission control implemented by the ISP backed up by the potential for liability on the ISP, it would shift the costs of UCEs away from recipients and towards the sender.

Nevertheless, any blocking mechanism should be implemented and supervised by authorities.[151] Recognizing ISPs' role as the gatekeeper for spammers to transmit UCEs, ISPs could be an effective tool to block the transmission of UCEs' that do not comply with transparency requirements. Due to ISPs' control over the transmission of information, service providers may abuse their power by leveraging their influence and blocking out their competitors. For example, an ISP with dominant market share may implement a block list that would allow its own commercial message to go through its filters while at the same time blocking UCEs of its competitors. Thus, in order to address this anti-competitive concern, block lists created by ISPs should be regulated by authorized governmental authorities.

C. *Necessity for International Cooperation in the Effort to Regulate UCEs*

Due to the borderless nature of the Internet, UCEs are routinely transmitted across national boundaries. A globally consistent spam regulation is effective in solving the problems presented by UCEs. This argument can be proven by the US experience with UCE regulation. State-by-state regulation of spam created inefficiencies. Divergent state legislation created the potential for loopholes that spammers use for forum shopping to avoid liability, which could diminish the effectiveness of political process. Therefore, a consistent international legal standard is desirable to avoid the problem of forum shopping.[152]

Nevertheless, a concern of high transaction costs associated with the political process in establishing an international legal standard or cooperation might not justify the participation in the international political

---

150. *Id.*

151. Matthew Sipe, *The Need for New Federal Anti-Spam Legislation*, 31 YALE J. ON REG. ONLINE 55, 58 (2014).

152. TRANS ATLANTIC CONSUMER DIALOGUE, RESOLUTION ON UNSOLICITED COMMERCIAL ELECTRONIC MAIL (2004), http://test.tacd.org/wp-content/uploads/2013/09/TACD-INTERNET-29-04-Unsolicited-Commercial-Electronic-Mail.pdf (last visited Oct. 23, 2015).

progress. Participation in the political process depend on the costs and benefits from the participants.[153] However, since seventy percent of all global e-mail traffic is spam, the benefits gained from freeing up usage and infrastructure loads to legitimate users, increasing productivity, and developing filtering technology outweighs the costs of government intervention. Given that UCEs are borderless in nature, the global benefits and costs should be taken into consideration as a whole. Through the efforts of various international organizations, such as OECD, APEC, and cross-national unions, such as the EU, countries may establish consistent legal standards for regulating UCEs. By allowing each country to incorporate these rules into domestic jurisdictions, international organizations could decrease the costs of participation in political process in each nation. Consequently, the inefficiencies created by differences between legal systems can be limited, resource allocation can be optimized, and online consumer protections can be strengthened.[154]

153. Neil K. Komesar, *The Essence of Economics: Behavior, Choice and Comparison—Essay One' the Basic Thesis with Lessons from the Economic Analysis of the Common Law*, 1173 UNIV. OF WISCONSIN LEGAL STUDIES RESEARCH PAPER 1, 10 (2011).

154. *Id*. (in order to provide consumers complete protection, TACD also encourages Internet services providers to provide better spam filter software, and inform consumers of their options and rights regarding UCEs).

REFERENCES

Akerlof, G. A. (1970). The Market for Lemon: Quality Uncertainty and the Market Mechanism. *Quarterly Journal Economics, 84*, 488-500.

America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D.Va. 1998).

America Online, Inc. v. National Health Care Discount, Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001).

Bread v. City of Alexandria, 341 U.S. 622 (1951).

Brown, E. (2015). Internet Law Regulatory and Litigation Matters. *Journal of Internet Law, 18*(7), 30-37.

California Business & Professional Code (2003).

Central Hudson Gas & Electronic Corp. v. Public Service Commission, 447 U.S. 557 (1980).

Charlesworth, A. (2003). Information Privacy Law in the European Union. *Hastings Law Journal, 54*, 931-969.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (2003).

Dayman D., Young, I. R. & Karwowski-Hoppel, C. A. (Jul. 29, 2008). *Japan New Anti-Spam Law*. Retrieved from http://www.mofo.com/news/updates/bulletins/14219.html.

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

Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 on Privacy and Electronic Communications, O.J. (L 201) 37 (2002).

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, O.J. (L 281) 31 (1995).

Elkin-Koren, N. & Salzberger, E. M. (2004). *Law, Economics and Cyberspace*. Northampton, MA: Edward Elgar Publishing, Inc.

Ellickson, R. C. (1989). The Case for Coase and Against "Coaseanism". *Yale Law Journal, 99*, 611-629.

Facebook, Inc. v. Wallace, No. C 09-798 JF (RS), 2009 WL 3617789 (N.D.Cal. Oct. 29, 2009).

Federal Trade Commission (2009). *The U.S. Safe Web Act, The First Three Year, Report to Congress.* Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/u.s.safe-web-a

ct-first-three-years-federal-trade-commission-report-congress/p035303safewebact2009.pdf.

Federal Trade Commission, Subject Line Labeling as a Weapon Against Spam (2005). Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/u.s.safe-web-act-first-three-years-federal-trade-commission-report-congress/p035303safewebact2009.pdf.

Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255 (Cal. App. 1st Dist. 2002).

First Keystone Federal Saving Bank v. First Keystone Mortgage, Inc., 923 F. Supp. 693 (E.D.Pa 1996).

Fisher, M. A. (2000). The Right to Spam? Regulating Electronic Junk Mail. *Columbia-VLA Journal of Law & the Arts, 23*, 363-418.

Florida Bar v. Went For It, Inc. 515 U.S. 618 (1995).

Fogo, C. E. (2000). The Postman Always Rings 4,000 Times: New Approaches to Curb Spam. *John Marshall Journal of Computer & Information Law, 18*, 915-944.

Graydon, S. M. (2000). Much Ado about Spam: Unsolicited Advertising, the Internet, and You. *Saint Mary's Law Journal, 32*, 77-114.

Gudkova, D. (2013). *Spam in Q2 2013*. Retrieved from https://securelist.com/analysis/quarterly-spam-reports/37148/spam-in-q2-2013/.

Harrison, J. L. (1995). *Law and Economics in a Nutshell.* Saint Paul, MN: West Group.

Hayward, C. L. (Ed.) (2004). *Identity Theft*. New York, NY: Novinka Books.

Hiramatsu, H. (2007). *Japan's Countermeasures Against Spam, Ministry of Internal Affairs and Communications, Japan.* Retrieved from http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/070410_2.pdf.

Khong, D. W. K. (2004). An Economic Analysis of Spam Law. *Erasmus Law & Economics Review, 1*, 23-45.

Komesar N. K. (2011). The Essence of Economics: Behavior, Choice and Comparison－Essay One "the Basic Thesis with Lessons from the Economic Analysis of the Common Law". *Univ. of Wisconsin Legal Studies Research Paper, 1173*, 1-29.

Komesar, N. K. (1994). *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy*. Chicago, IL: University of Chicago Press.

Magee, J. (2003). The Law Regulating Unsolicited Commercial E-mail: An International Perspectives. *Santa Clara Computer & High Technology Law Journal, 19*, 333-382.

Mansfield, E. (5th ed. 1985). *Micro-Economics: Theory and Application*. New York: Norton.

Marsden, C. T. (2001). Cyberlaw and International Political Economy: Towards Regulation of the Global Information Society. *Law Review of Michigan State University-Detroit College of Law, 2001*, 355-382.

Missouri ex rel. Nixon v. American Blast Fax, Inc., 323 F.3d 649 (8th Cir. 2003).

Mobarek, S. I. (2004). The Can-Spam Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to It?. *Loyola Consumer Law Review, 16*, 247-266.

Moorefield, G. S. (1999). SPAM－It's Not Just for Breakfast Anymore: Federal Legislation and the Flight to Free the Internet from Unsolicited Commercial E-mail. *Boston University Journal of Science & Technology Law, 5*, 1-45.

Mutchler, A. (2010). Can-Spam Act Versus the European Union E-Privacy Directive: Does Either Provide a Solution to the Problem of Spam. *Suffolk University Law Review, 43*, 957-981.

Organization for Economic Co-operation and Development (2003). *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*. Retrieved from http://www.oecd.org/sti/ieconomy/37125909.pdf.

Overby, A. B. (2001). An Institutional Analysis of Consumer Law. *Vanderbilt Journal of Transnational Law, 34*, 1219-1291.

Overview of Japan Anti-Spam Law. *Ministry of Internal Affairs and Communications in Japan*, Retrieved from http://measures.antispam.go.jp/pdf/overview%20of%20Japanese%20anti-spam%20law.pdf.

Pandya, M., Shell, R., Warner, S., Junnarkar, S. & Brown, J. (2004). *Nightly Business Report Presents Lasting Leadership: What You Can Learn from the Top 25 Business People of Our Times*. Upper Saddle River, NJ: Tim Moore.

Phlips, L. (1983). *The Economics of Price Discrimination.* Cambridge, UK: Cambridge University Press.

Radicati, S. (Ed.) (2009). *E-mail Statistics Report, 2009-2013*. Retrieved from http://www.radicati.com/wp/wp-content/uploads/2009/05/e-mail-stats-report-exec-summary.pdf.

Radin, M. J. et al. (2002). *Internet Commerce: The Emerging Legal Frameworks*. New York: Foundation Press.

Rao, J. M. & Reiley, D. H. (2012).The Economics of Spam. *Journal of Economics Perspectives*, *26*(3), 87-110.

Ribstein, L. E. & Kobayshi, B. H. (2002). State Regulation of Electronic Commerce. *Emory Law Journal, 51*, 1-80.

Rosolowski v. Guthy-Renker LLC, No. B250951 (Cal. Ct. App. Oct. 29, 2014).

Rosolowski v. People Media, Inc., No. B250482, 2014 WL 5472450 (Cal. Ct. App. Oct. 29, 2014).

Schultz, J. (2014, May 2). Spam Hits Three Year High-Water Mark, *Cisco Blogs*. Retrieved from http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark.

Sipe, M. (2014). The Need for New Federal Anti-Spam Legislation. *Yale Journal on Regulation Online, 31*, 55-59.

Smith, A. (1911). *The Wealth of Nations*. New York, NY: P.F. Collier & Son. Publishing.

Soma, J., Singer, P. & Hurd, J. (2008). Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions. *Harvard Journal on Legislation, 45*, 165-198.

Spam and Phishing Statistics Report Q1-2014, *Kaspersky Lab*. Retrieved from http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014#.VTkFCGSeAXB.

State Laws Relating to Unsolicited Commercial or Bulk E-Mail (SPAM), NAT'L CONF. OF ST. LEGIS. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/state-spam-laws.aspx.

State v. Heckel, 24 P.3d 404 (Sup. Ct. WA. 2001).

Tatyana Shcherbakova & Maria Vergelis (Sept. 23, 2013, 03:05 am). *Spam in August 2013, Securelist*. Retrieved from http://www.securelist.com/en/analysis/204792306/Spam_in_August_2013#7.

Tokutei Denshi Mēru no Sōshin no Tekisei-ka-tō ni Kansuru Hōritsu (2009). [Act on Regulations of the Transmission of Specified Electronic Mail] (Japan) Retrieved from http://measures.antispam.go.jp/pdf/Japanese%20anti-spam%20law.pdf.

Tokutei Denshi Mēru no Sōshin no Tekisei-ka-tō ni Kansuru Hōritsu Shikōkisoku (2002). [Ordinance for Enforcement of the Act on

Regulation of the Transmission of Specified Electronic Mail] (Japan), Retrieved from http://measures.antispam.go.jp/pdf/Ordinance%20for%20Enforcement%20of%20the%20Act%20on%20Regulation%20of%20the%20Transmission%20of%20Specified%20Electronic%20Mail.pdf.

Trans Atlantic Consumer Dialogue (2004). *Resolution on Unsolicited Commercial Electronic Mail*. Retieved from http://test.tacd.org/wp-content/uploads/2013/09/TACD-INTERNET-29-04-Unsolicited-Commercial-Electronic-Mail.pdf.

Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2006 (2006).

Verizon Online Services, Inc. v. Ralsky, 203 F. Supp. 2d 601 (E.D.Va. 2002).

Zerbe, R. O. Jr. (2001). *Economic Efficiency in Law and Economics*. Northampton, MA: Edward Elgar Pub. Rosenthal.

Zhang, L. (2005). The CAN-Spam ACT: An Insufficient Response to the Growing Spam Problem. *Berkeley Technology Law Review, 20*, 301-332.

規範網路垃圾郵件之機構選擇分析

石 佳 立

摘 要

網際網路提供快速資訊流通及跨國界的管道，如此的管道對於資訊之傳播宛如一刀兩面，利弊兼具。自動發出的商務電子郵件，通稱「垃圾郵件」，係指未經電子郵件用户之許可，透過所取得的電子郵件名冊，以寄送商業行銷資訊為目的，廣泛、大量的寄出電子垃圾郵件。垃圾郵件之傳播係利用網際網路的特性，以達到快速及有效率的行銷方式，但是垃圾郵件同時也造成相當的負面外部成本，更甚者，垃圾郵件亦造成全球性的網際網路隱私權以及線上安全的衝擊。

因此本文採用法律與經濟分析的方法，以釐清特定適當的機構選擇，以達到發揮垃圾郵件的效益以及降低其所帶來的外部成本。本文同時比較現今美國、歐盟以及日本關於垃圾郵件的規範，藉由比較法之研究與分析，提出國際立法合作以規範垃圾郵件的架構。

關鍵詞：垃圾郵件、機構選擇、美國垃圾郵件法、法律經濟分析、網路行銷