Privacy Regulation

Summer 2002

Table of Contents

Consumer Protection Committee
Computer and Internet Committee
Section of Antitrust Law
American Bar Association
750 North Lake Shore Drive
Chicago, Illinois 60611

Privacy Regulation

Summer 2002

Privacy Regulation is published two times a year by the American Bar Association Section of Antitrust Law Consumer Protection and Computer and Internet Committees. The views expressed in the Newsletter are the authors' only and not necessarily those of the American Bar Association, the Section of Antitrust Law, or the Consumer Protection and Computer and Internet Committees (or their subcommittees).

If you wish to comment on the contents of the Newsletter, please write to the American Bar Association, Section of Antitrust Law, 750 North Lake Shore Drive, Chicago, IL 60611.

From the Editor

The ABA Section of Antitrust Law's Consumer Protection and Computer and Internet Committees are pleased to present Privacy Regulation, their new privacy law newsletter. This publication, which will be delivered by email semiannually to members of both Committees who have registered for their respective Committee's Listserves, will focus on specific, timely privacy issues. This issue addresses the regulation of unsolicited commercial email in three articles. Jeff Kauffman, of Collier Shannon Scott, addresses U.S. federal regulation; Vanessa Nelson, of Dreher Langer & Tomkies L.L.P., focuses on U.S. state law regulation; and Rachael Wellby of Crowell & Moring's London office addresses EU laws regulating unsolicited commercial email. The next issue, targeted for publication in February, will focus on developing and implementing a globally-compliant privacy policy. If you would like to submit an article for that issue, please send your proposal to me at rfreeman@colliershannon.com.

This new publication could not have been possible without the untiring support of David Evans, Co-Chair of the Computer and Internet Committee, who proposed this newsletter, recruited the Editorial Board, and provided the leadership necessary to make this publication a reality; and Robert Langer, Chair of the Consumer Protection Committee, who provided his invaluable guidance and advice. Members of the Editorial Board – David Evans of Jones Day's DC office; Peder Magee, Attorney Advisor to FTC Commissioner Mozelle Thompson, and John Villafranco and Elisa Nemiroff, both of Collier Shannon – have also worked hard to make sure that the articles we publish are accurate, complete and, most importantly, focused on assisting privacy law practitioners in their day-to-day work.

We hope that you will find this newsletter useful in your practice. If you have any questions, comments, or suggestions for improvement of this newsletter, please let me know.

D. Reed Freeman, Jr.
Collier Shannon Scott PLLC
Washington, DC
rfreeman@colliershannon.com

Privacy
Regulation
Summer 2002

Taking a Bite Out of Spam: The EU Opts for "Opt-In"

Rachael Wellby[1]
Crowell & Moring
London
rwellby@crowell.com

The pace at which people have come to rely on email as a means of business and personal communication is perhaps exceeded only by the explosive growth of unsolicited commercial email ("UCE") as a means of direct marketing. Although it is simple to decry the proliferation of "spamming," it is also simplistic. Distinguishing between acceptable and unacceptable uses of UCE — in essence, defining what constitutes "spam" — is not easy.[2] Just as difficult perhaps, is determining the appropriate methods of controlling UCE. One of the key policy issues confronting the business communities and regulatory agencies around the world is the extent to which a recipient's consent (or at least acquiescence) to receive UCE should be required. Although the debate between "opt-out" and "opt-in" schemes continues in the United States, the European Parliament recently took steps to resolve the issue directly, coming down on the side of requiring "opt-in" — but only in certain circumstances.

At present, the use of UCE in Europe may be subject to indirect regulation under three separate, but related EU Directives: the Data Protection Directive;[3] the e-Commerce Directive;[4] and, in some countries, the Telecommunications Directive.[5] Recently, however, the European Parliament approved the Electronic Communications Directive,[6] which addresses UCE explicitly. By the end of 2003, EU Member States likely will have implemented laws consistent with the new Directive. This article briefly examines the current EU regulatory scheme, as well as the changes that will be implemented as the Electronic Communications Directive goes into effect.

EU Directives and National Law

The European Union, which comprises 15 Member States,[7] was founded with the aim of establishing a customs union to achieve the free flow of goods, capital and labour within a single European market. The Euro-

pean Commission acts as the executive arm of the EU, and has the power to submit proposals for future legislation — including Directives — to the Council of Ministers and the European Parliament. Proposed Directives follow a complex path of readings, amendments and voting in passing through both the Council of Ministers (which consists of ministerial level representatives from each Member State), and the European Parliament (which is the EU's only directly elected institution). Directives that successfully negotiate passage through these institutions will return to the Commission in order to be formally adopted.

Final EU Directives establish the essential features of subject matter legislation, and direct each Member State to transpose those measures into national law by a specified implementation date. Directives are binding on Member States and the European Commission, through the European Court of Justice, may fine Member States that fail to take necessary measures to enact a Directive's provisions by the specified date.

Frequently, as is the case with the Electronic Communications Directive, EU Directives are silent as to the scope of their jurisdictional application. In these instances, Member States must determine the scope of the laws passed to effectuate the terms of the Directive at the national level. Certain general jurisdictional rules do, however, continue to apply. For example, the "Brussels Regulation"[8] provides that a consumer may sue the other party to a contract in the consumer's place of domicile. Therefore, a consumer who is party to a contract with a foreign organization conducting direct marketing activities[9] may be able to sue that organization in the consumer's own country for non-compliance with national law.[10] The Brussels Regulation does not extend jurisdiction over consumer claims against entities with whom the consumer has no contract; consequently, it does not provide local jurisdiction for consumer actions against spammers.

Current EU Regulation of UCE

-The Data Protection Directive

The Data Protection Directive protects the use of "personal data," which is defined as information that identifies or enables identification of an individual.[11] Although this Directive does not focus on email in particular, an email address (either by itself or in conjunction with other information) can constitute personal data. An email address that identifies an individual's name and place of business, for example, could by itself be considered personal data if it were sufficient to identify the person. In other cases, the email address together with other information that a marketer might obtain, such as the individual's name and home address, likely would constitute personal data and therefore be subject to the Directive.

Data Protection Directive

Directive 1995/46/EC of the European Parliament and of the Council of 24 October 2000 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm.

E-Commerce Directive

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market, available at http://europa.eu.int/comm/internal_market/en/ecommerce/index.htm.

Under the Directive, personal data may only be used for a "specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes."[12] Specifically with regard to marketing uses of personal data (which would include, but certainly is not limited to, UCE), individuals have the right to object to the use of their data "for the purposes of direct marketing, and to be expressly offered the right to object . . . to such disclosures or uses."[13] Where an individual's email address constitutes personal data and was provided for a discrete purpose, such as an online purchase, any subsequent use of that email address for marketing purposes is prohibited absent disclosure by the marketer to the individual. Accordingly, UCE marketing activities must, at a minimum under the Data Protection Directive, offer the individual an opportunity to "opt-out" of further contact.

Although violation of the Data Protection Directive can be the basis for an award of damages, in most instances it likely would be difficult for an individual whose personal data was misused to show actual injury. Moreover, in many instances, spammers are difficult to locate. Consumer complaints may form the basis for action by a national supervisory authority, however. The Directive permits such an authority to take injunctive action to prohibit violative use of personal data and impose criminal sanctions on persistent offenders.

-The e-Commerce Directive

Pursuant to the e-Commerce Directive, Member States that allow UCE must "ensure that such [communication] shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient."[14] The Directive also requires Member States to ensure that marketers using UCE "consult regularly and respect the 'opt-out registers.'"[15] To some degree, the latter provision has been incorrectly interpreted as stating that an "opt-out" scheme is sufficient.[16] As discussed below, the Electronic Communications Directive explicitly addresses this issue.

-The Telecommunications Directive

The Telecommunications Directive bars unsolicited faxes and computerized marketing calls, requiring an entity to obtain prior consent from the recipient before using automated telephone or fax systems for direct marketing purposes. By requiring "prior consent," the Directive appears to advocate an "opt-in" scheme. However, critics have argued that the absence of express guidance left the door open for prior "opt-out" consent. By its terms, this Directive does not specifically govern direct marketing via UCE. Nonetheless, several Members States, including Austria, Denmark, Finland and Italy, have, in implementing the Telecommunications Directive into their national laws, explicitly extended these provisions to include electronic mail.

Telecommunications Directive

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, available at http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm.

Electronic Communications Directive

Directive 2002/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at http://europa.eu.int/eur-lex/en/dat/2002/l_201/l_20120020731en00370047.pdf

The Electronic Communications Directive

On May 30, 2002, the European Parliament approved the Electronic Communications Directive, which Member States likely will be required to implement into their national law by December 2003. Once implemented, the Directive will repeal and replace the Telecommunications Directive, since telecommunications activities are encompassed within the broader definition of electronic communications.

As a general rule, the Electronic Communications Directive prohibits direct marketing via electronic mail (including SMS messaging) unless the intended recipient has given prior consent to receive such communications.[17] The Directive's recitals provide clarity that consent must be "opt-in," specifying that consent must be a "freely given, specific and informed indication of the user's wishes," and that consent may be provided, by way of example, "by ticking a box when visiting an Internet website."[18] There is an important exception, however, intended to limit the effect of the requirement to spammers. Under the Directive, prior consent is not required if the communication is made to existing customers for the purpose of offering similar products or services.[19] Accordingly, businesses communicating with existing customers in many circumstances will be able to rely on an "opt-out" consent.

The Directive targets spammers by prohibiting UCE that conceals the identity of the sender or does not have a valid return address.[20] This prohibition is intended to "facilitate effective enforcement of rules on unsolicited messages for direct marketing."[21] In addition, the Directive's recitals encourage the development of email systems that contain technical measures allowing subscribers to view the sender and subject lines of emails and delete the message without viewing it in full or downloading it. This is seen as a useful tool in "reducing costs which could arise from downloading unsolicited electronic mails or attachments."[22] The Directive envisages that measures "may be adopted" in the future to ensure that "terminal equipment is constructed in a way that is compatible with the rights of users to protect and control the use of their personal data."[23]

Although the nature of the mechanisms that Member States are likely to establish in order to facilitate effective enforcement of the Directive are currently unknown, the European Union's intentions in this regard are clear. Article 17a of the Directive provides that the European Commission must, within three years, report to the European Parliament and Council on the implementation and impact of the Directive "in particular as regards the provisions of unsolicited communications." The Commission is also instructed, based upon the results of the report, to submit appropriate proposals to amend the Directive as maybe required "in order to improve [its] effectiveness." Therefore, should any Member State fail to implement enforcement mechanisms sufficiently robust to achieve the aims of the Directive and reduce the level of UCE, we are likely to see amendments to enforcement schemes within a matter of years.

Conclusion

The Electronic Communications Directive imposes no new consent requirements on a company sending UCE to its current customers as the Data Protection Directive already requires notice and consent (express or implied) before such expanded use of a customer's personal data is permitted. A policy of openness about the uses to which customers' email addresses will be put, coupled with providing clear opportunities to "opt-out" of direct marketing, will thus go a long way towards satisfying Europe's UCE requirements with respect to existing customers.

But where no customer relationship exists, businesses will be required by the new Electronic Communications Directive to obtain prior "opt-in" consent before commencing any unsolicited direct marketing activities. It remains to be seen whether this provision, which has the effect of prohibiting spamming, will stop the current surge of UCE. Ultimately, the success of the Electronic Communications Directive in reducing UCE will be determined largely by the extent to which individual Member States choose to incorporate strong enforcement mechanisms into their national laws implementing its provisions.

(Endnotes)

1 Rachael Wellby (rwellby@crowell.com, 011 44 20 7413-0070) is an associate in Crowell & Moring's London office. Before joining Crowell, she worked with the OECD in Paris on international policy issues concerning online privacy and the development of an online privacy policy generator. She was assisted in the preparation of this article by Jonathan Fitzgibbons (jfitzgibbons@crowell.com, 011 44 20 7413-1319) and John Stewart (jstewart@crowell.com, 202-624-2685), who is the chair of the firm's Technology, Media, and Telecommunications Group, based in the Washington, D.C., office of Crowell & Moring.

2 It has been said that "one person's spam is another person's meat and potatoes."

3 Directive 1995/46/EC of the European Parliament and of the Council of 24 October 2000 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market.

5 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

6 Directive 2002/EC of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

7 The EU Member States are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, Ireland, Luxembourg, The Netherlands, Portugal, Spain, Sweden and the United Kingdom. In addition, thirteen countries recently applied for EU membership and are currently taking steps to meet the so-called "accession criteria." These accession countries include Turkey, Cyprus, Malta, Hungary, Poland, Romania, Estonia, Lithuania, Bulgaria, Czech Republic, Slovak Republic, Latvia, and Slovenia.

8 Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, 1968.

9 A "consumer" is one who concludes a contract for a purpose outside his trade or profession with a person who either pursues commercial or professional activities in the member state of the consumer's domicile or by any means directs such activities to that member state.

10 Provided the national law creates a consumer cause of action.

11 Article 2(a), the Data Protection Directive.

12 Id. Article 6(b).

13 Id. Article 14(b).

14 Id. Article 6(a), the e-Commerce Directive.

15 Id. Article 7(2).

16 Unsolicited Commercial Communications and Data Protection, Gauthronet and Drouord, European Commission, 2001.

17 Article 13, the e-Commerce Directive.

18 Paragraph 17, Preamble, the Electronic Communication Directive.

19 Article 13, the Electronic Communications Directive.

20 Id.

21 Id. Recital 43, the Electronic Communications Directive.

22 Id. Recital 44a.

23 Id. Article 14.

Privacy
Regulation
Summer 2002

Use of UCE: An Overview of State Laws Regarding Unsolicited Commercial Electronic Mail Advertisements

Vanessa A. Nelson*
Dreher Langer & Tomkies LLP
Columbus, OH
vnelson@dltlaw.com

Introduction

The gradual decline in the effectiveness of direct mail solicitations coupled with recent concerns about anthrax and postal rate hikes has sparked an increased interest in alternate means of advertising, including electronic mail ("email"). For various reasons, however, many consumers view unsolicited commercial email ("UCE") (also known as "spam" or "junk email") as an unwelcome intrusion. Email service providers are also wary of the burdens associated with UCE. In recognition of these concerns and to create protections from abusive email practices, many states have enacted "anti-spam" legislation.

As of July 2002, 25 states have enacted UCE laws, most of which are applicable to commercial entities that use email to advertise products or services to consumers.[1] This article provides a general overview of these state laws, outlines available exemptions from their requirements, discusses affirmative compliance obligations, and highlights enforcement issues regarding these laws.

I. General Categories of State UCE Laws

In general, the state statutes governing UCE can be divided into three loose and somewhat overlapping categories: "anti-fraud," "opt-out," and "email service provider protection."

A. Anti-Fraud

Approximately one-half of state UCE laws (including Arkansas, Connecticut, Illinois, Louisiana, Maryland, North Carolina, Oklahoma, Rhode Island,[2] South Dakota, Virginia, Washington, and West Virginia) are designed to deter fraud by prohibiting the sending of commercial emails

that contain falsified or forged information in the source, point of origin (i.e., the identity of the sender), transmission path (i.e., how the electronic message traveled from the sender's outbox to the recipient's inbox), or subject line. Many of these statutes (including Arkansas, Illinois, Maryland, South Dakota, Washington, and West Virginia) also prohibit the use of a third party's Internet domain name without the third party's permission. The "anti-fraud" category of statutes does not impose any other specific content requirements, so compliance with these laws should be relatively easy.

B. Opt-Out

Approximately one-half of state UCE laws (including California, Colorado, Delaware, Idaho, Iowa, Kansas, Minnesota, Missouri, Nevada, Rhode Island, Tennessee, and Utah) require email marketers to provide consumers with the option of declining receipt of future UCE. Although the Delaware UCE law is included within this category of statutes, it is unique in that it also generally prohibits UCE.[3] These statutes (which may also include anti-fraud provisions (discussed above) and/or service provider protection provisions (discussed below)), generally require that UCE messages include a toll-free telephone number or email address within the body of the email to enable consumers to opt-out of receipt of future UCE, and prohibit sending UCE to those individuals who have previously exercised their right to opt-out. The "opt-out" category of statutes poses more of a compliance challenge because these regulations are more detailed and less uniform than the "anti-fraud" type.

C. Email Service Provider Protection

Many email service providers are concerned that the sheer volume of UCE mailings may overburden their computer systems, potentially disrupting service to their registered members and/or damaging their equipment. Thus, nearly half of state UCE laws (including California, Delaware, Iowa, Kansas, Louisiana, Maryland, Minnesota, North Carolina, Rhode Island, South Dakota, Virginia, and West Virginia) include measures designed to protect email service providers. Some of these laws prohibit the sending of emails without authorization or in violation of policies established by the email service provider.[4] Other service provider-oriented laws, such as Maryland's Commercial Electronic Mail statute and Kansas's Commercial Electronic Mail Act, provide that an email service provider may block the receipt or transmission of commercial email that it reasonably believes is or will be sent in violation of the state UCE statute. These laws shield the email service provider from liability for voluntarily and in good faith blocking such messages.[5] In light of these laws, email marketers should ensure that their use of UCE is consistent with their email service providers' policies and applicable state laws.

List of State UCE Laws

1. **Arkansas**: Computer Crimes, Ark. Code Ann. § 5-41-201.

2. **California**: Faxing or Emailing of Unsolicited Advertising Materials, Cal. Bus. & Prof. Code § 17538.4;[13] Electronic Mail Service Providers, Cal. Bus. & Prof. Code § 17538.45.

3. **Colorado**: Colorado Junk Email Law, Colo. Rev. Stat. Ann. § 6-2.5-101 et seq.

4. **Connecticut**: Computer Crimes, Conn. Gen. Stat. Ann. § 53-451 et seq.

5. **Delaware**: Computer Related Offenses, Del. Code Ann. tit. 11, § 931 et seq.

6. **Idaho**: Unfair Bulk Electronic Mail Advertising Practices, Idaho Code § 48-603E.

7. **Illinois**: Electronic Mail Act, 815 ILCS 511/1 et seq.

8. **Iowa**: Electronic Mail Transmissions, Iowa Code § 714E.1 et seq.

9. **Kansas**: Commercial Electronic Mail Act, Kan. Stat. Ann. § 1(e), (f), enacted by 2002 Kan. S.B. 467 (effective upon publication in the statute book).

10. **Louisiana**: Computer Related Crime, La. Rev. Stat. Ann. § 14:73.1 et seq.

11. **Maryland**: Commercial Electronic Mail, Md. Code Ann., Com. Law, § 14-2901 et seq., enacted by 2002 Md. S.B. 538 (effective Oct. 1, 2002).

List of State UCE Laws (con't)

12. **Minnesota**: Commercial Electronic Mail Solicitation, Minn. Stat. Ann. § 325F.694, enacted by 2002 Minn. S.F. 2908.

13. **Missouri**: Electronic Mail Practices, Mo. Rev. Stat. Ann. § 407.1120 et seq.

14. **Nevada**: Liability of Persons Who Transmit Items of Electronic Mail That Include Advertisements, Nev. Rev. Stat. Ann. § 41.705 et seq.

15. **North Carolina**: Computer-Related Crime, N.C. Gen. Stat. § 14-453 et seq.; Damages for Computer Trespass, N.C. Gen. Stat. § 1-539.2A.

16. **Oklahoma**: Fraudulent Electronic Mail, Okla. Stat. Ann. tit. 15, § 776.1 et seq.

17. **Pennsylvania**: Sexually Explicit Materials, 18 Pa. Cons. Stat. Ann. § 5903.

18. **Rhode Island**: Unsolicited Electronic Mail, R.I. Gen. Laws § 6-47-2; Computer Crime, R.I. Gen. Laws § 11-52-1 et seq.

19. **South Dakota**: Misleading Unsolicited Commercial Emails, S.D. Codified Laws Ann. § 37-24-1 et seq., enacted by 2002 S.D. S.B. 180 and 2002 S.D. S.B. 183.

20. **Tennessee**: Unsolicited Advertising by Electronic Means, Tenn. Code Ann. § 47-18-2501 et seq.

II. Scope and Exemptions

A. Jurisdictional Scope

One of the advantages of email is the ability to distribute advertisements quickly and inexpensively nationwide. However, because a state's jurisdiction over email senders usually depends upon the recipients' location(s), senders may not know which state's law applies to any given message. Even if a sender can sort mailing lists by recipients' state of residence, senders may never be certain where recipients actually receive these messages. Given this geographic uncertainty, a conservative email marketer should comply with all state UCE laws, unless a relevant exemption exists.

B. Exemptions from State UCE Laws

There are at least four exemptions potentially available to a commercial email advertiser. First, 12 states (California, Colorado, Delaware, Illinois, Kansas, Minnesota, Missouri, Nevada, North Carolina, Rhode Island, South Dakota, and Utah) provide an exemption for messages sent to persons with whom the sender has a prior or existing business relationship. Second, messages sent at the request or with the consent of the recipients are exempt in 13 states (Arkansas, California, Colorado, Delaware, Illinois, Kansas, Minnesota, Nevada, North Carolina, Rhode Island, South Dakota, Utah, and West Virginia). Third, 10 states (including Colorado, Connecticut, Delaware, Idaho, Iowa, Louisiana, Minnesota, Rhode Island, Tennessee, and Virginia) exempt messages from organizations using email to communicate exclusively with their members. Finally, six states (including Idaho, Iowa, Maryland, Missouri, South Dakota, and Washington) exempt email sent to certain free email accounts. For example, Idaho's Unfair Bulk Electronic Mail Advertisement Practices statute does not apply to a "person who provides users with access at no charge to electronic mail, including receiving and transmitting bulk electronic mail advertisements, and, as a condition of providing such access, requires such users to receive unsolicited advertisements."[6] If an email marketer is unable to avail itself of these exemptions, it may be subject to the following requirements and limitations.

III. Requirements and Limitations

A. "Do Not Email"

Nine states (California, Colorado, Delaware, Idaho, Iowa, Kansas, Rhode Island, Tennessee, and Utah) prohibit entities from sending email communications to persons who have requested to receive no further UCE. The state UCE laws of Utah and California contain some unique variations on the "do not email" theme. The Utah Unsolicited Commercial Email Act specifies that senders may not email those who have opted out either directly or through a subsidiary or affiliate.[7] The Utah law also

appears to require affiliated companies to maintain centralized "do not email" lists. California law contains a provision that allows an employer who is the registered owner of more than one email address to notify a person or entity conducting business in California to cease emailing unsolicited advertising material to all employees who use employer-provided email addresses.[8]

List of State UCE Laws (con't)

21. **Virginia**: Computer Crimes, Va. Code Ann. § 18.2-152.1 et seq., amended by 2002 Va. H.B. 304.

22. **Utah**: Unsolicited Commercial Act, Utah Code Ann. § 13-34-101 et seq., enacted by 2002 Utah S.B. 143 (effective May 6, 2002); Unsolicited Commercial and Sexually Explicit Email Act, Utah Code Ann. § 13-34-101 et seq., enacted by 2002 Utah H.B. 143.

23. **Washington**: Commercial Electronic Mail, Wash. Rev. Code Ann. §§ 19.190.010 et seq.[14]

24. **West Virginia**: Electronic Mail Protection Act, W.Va. Code § 46A-6G-et seq.

25. **Wisconsin**. Sending Obscene or Sexually Explicit Messages, Wis. Stat. Ann. § 944.25.

B. Opt-Out Disclosures

To facilitate "do not email" requests, the laws in 12 states (California, Colorado, Delaware, Idaho, Iowa, Kansas, Minnesota, Missouri, Nevada, Rhode Island, Tennessee, and Utah) explicitly prohibit the sending of email messages that do not contain a toll-free telephone number and/or return email address to enable consumers to opt out of receiving future communications. For example, Nevada law, which perhaps contains the most specific requirements, provides that a person who transmits or causes to be transmitted an email advertisement may be liable to the recipient unless, *inter alia*, "the advertisement is readily identifiable as promotional, or contains a statement providing that it is an advertisement and clearly and conspicuously provides: (1) the legal name, complete street address and email address of the person transmitting the email. . . ."[9]

Moreover, seven states (California, Delaware, Kansas, Minnesota, Rhode Island, Tennessee, and Utah) require that senders of commercial email include within the body of the email message a statement notifying consumers of their right to opt out of future solicitations. In California, this statement must be the first text in the body of the message and of the same size as the majority of the text.[10]

C. Subject Line

Eight states (Arkansas, Illinois, Kansas, Maryland, Minnesota, South Dakota, Washington, and West Virginia) prohibit email marketers from including false, misleading, or malicious information in subject lines. Seven states (California, Colorado, Kansas, Minnesota, South Dakota, Tennessee, and Utah) require that the characters "ADV:" precede any other text in the subject line of an advertisement. In addition, if the email message contains unsolicited advertising material for the lease, sale, rental, gift offer or other disposition of any realty, goods, services or extension of credit that may only be viewed, purchased, rented, leased or held in possession by an individual 18 years of age and older, California, Iowa, South Dakota, and Tennessee laws require that "ADV: ADLT" appear as the first characters of the subject line.

D. Identifying Information

Unscrupulous email marketers often attempt to evade detection by omitting, misrepresenting, or falsifying the point of origin or other transmission information associated with their email messages. Most state UCE

laws prohibit the sending of emails that fail to contain accurate and complete information regarding the identity of the sender and/or transmission information.

IV. Enforcement/Penalties

The state UCE statutes contain various enforcement and penalty provisions. Most states (with the exception of Arkansas, Louisiana, and Virginia) allow a private right of action for damages.[11] Some states explicitly permit class actions (Idaho and Missouri) and/or the award of punitive (Idaho and West Virginia) or treble (Delaware and South Dakota) damages. Class actions are specifically prohibited by Minnesota law.[12] Civil penalties may be imposed in a few states (such as California, Colorado, Illinois, Kansas, Missouri, and Oklahoma). Injunctive and other equitable relief, attorneys' fees, and/or costs are also available in the majority of states (with the exception of Arkansas, Kansas, Louisiana, and Virginia). Finally, state UCE law violations can result in criminal fines and/or imprisonment in a handful of states (such as Arkansas, California, Colorado, Connecticut, Delaware, Louisiana, Missouri, North Carolina, and Virginia).

Conclusion and Keys to Minimizing Risk

The good news about state UCE laws is that, although there are multiple state laws with differing requirements, the combined compliance costs are relatively low and the restrictions are generally manageable. The keys to minimizing the risk of advertising by email are (i) keeping current with existing state UCE laws and new legislation, (ii) drafting email advertisements with state law requirements in mind, (iii) following email service providers' UCE policies or guidelines, (iv) establishing and updating opt-out lists and (v) honoring opt-out requests.

The keys to minimizing the risk of advertising by email are:

(i) keeping current with existing state UCE laws and new legislation,

(ii) drafting email advertisements with state law requirements in mind,

(iii) following email service providers' UCE policies or guidelines,

(iv) establishing and updating opt-out lists and

(v) honoring opt-out requests.

(Endnotes)

* Vanessa A. Nelson is an associate with Dreher Langer & Tomkies L.L.P., a Columbus, Ohio law firm concentrating in the area of banking and financial services, and is an editor of the Firm's Marketing and Privacy Digest. She can be reached at vnelson@dltlaw.com. This article reflects the personal views of the author. It has been prepared for informational purposes only and so does not constitute legal advice. This publication is not intended to create, and the receipt of it does not create, an attorney-client relationship.

1 Pennsylvania, Utah, and Wisconsin have enacted laws regarding the dissemination of explicit sexual material via email. These laws are beyond the scope of this article.

2 Rhode Island has two UCE statutes, one of which (Computer Crime) is in the "anti-fraud" category and the other (Unsolicited Electronic Mail) is in the "opt-out" category.

3 Del. Code Ann. tit. 11, § 937(1).

4 *See*, *e.g.*, La. Rev. Stat. Ann. § 14:73.6(A); N.C. Gen. Stat. § 14-458(a)(6); W. Va. Code §§ 46A-6G-1(1), 46A-6G-5(a).

5 *See*, *e.g.*, Md. Code Ann., Com. Law, § 14-2902(d), *enacted by* 2002 Md. S.B. 538 (effective Oct. 1, 2002); 2002 Kan. S.B. 467, § 1(e), (f) (effective upon publication in the statute book).

6 Idaho Code § 48-603E(5)(c).

7 Utah Code Ann. § 13-34-103(3), *enacted by* 2002 Utah H.B. 80, § 3.

8 Cal. Bus. & Prof. Code § 17538.4(h).

9 Nev. Rev. Stat. Ann. § 41.730(1)(c).

10 Cal. Bus. & Prof. Code § 17538.4(b).

11 The private right of action is available to a recipient in 10 states (Colorado, Idaho, Maryland, Missouri, Nevada, Rhode Island, South Dakota, Utah, Washington, and West Virginia), to a service provider in 10 states (California, Colorado, Connecticut, Maryland, Missouri, North Carolina, South Dakota, Utah, Washington, and West Virginia), or to any person injured by UCE in violation of a statute in 10 states (Connecticut, Delaware, Illinois, Iowa, Kansas, Maryland, Minnesota, North Carolina, Oklahoma, and Tennessee).

12 Minn. Stat. Ann. § 325F.694, Subd. 7(e), *enacted by* 2002 Minn. S.F. 2908 (effective Mar. 1, 2002).

13 This statute has been upheld against a constitutional challenge. *See Ferguson v. Friendfinders, Inc.*, 94 Cal. App. 4th 1255 (2002) (holding that the California statute governing UCE does not violate the dormant Commerce Clause of the United States Constitution).

14 This statute also has been upheld against a constitutional challenge. *See State v. Heckel*, 143 Wash. 2d 824 (2001), *cert. denied*, 122 S.Ct. 467 (2001) (holding that the Washington Commercial Electronic Mail Act does not violate the dormant Commerce Clause of the United States Constitution).

Privacy
Regulation
Summer 2002

You've Got Mail...And More Mail...And More Mail: Federal Regulation of Unsolicited Commercial Email

Jeffrey A. Kauffman
Collier Shannon Scott PLLC
Washington, DC
jkauffman@colliershannon.com

"The magic of email is that you can email almost anyone. The tragedy is that almost anyone can email you."[1]

The reality of this statement is realized by millions. Unsolicited commercial email, also known as "spam" or "UCE," is a daily irritant that clogs inboxes. But beyond the annoyance spam creates, there are additional concerns. A large number of unidentifiable spammers send false and misleading emails to consumers without fear of legal penalty, consumers expend valuable connection time deleting spam and unsuccessfully attempting to unsubscribe from mailings lists, and businesses incur costs, both in having to add network capacity and security protection against viruses, and trojan horses, and in the decreased productivity of employees who must deal with spam.

Recently, the federal government has shown an interest in curtailing spam. In an effort to direct some of the costs back to the spammers in the form of civil and criminal penalties, and to limit the flow of deceptive UCE, the Federal Trade Commission ("FTC") has taken a number of enforcement actions and engaged in several public education programs. In addition, proposed federal legislation would provide regulators with the additional authority needed to reduce the amount of spam that we receive each day.

The Costs

In January 2002, spam accounted for an estimated 11 to 26 percent of all email traffic on the Internet, up 46 percent from the previous year.[2] America Online, the nation's largest Internet Service Provider ("ISP"), has estimated that spam accounts for 30 percent of its email traffic.[3] Not only is spam increasing, but so is its file size. This increase in size will require more servers and additional storage space.

This increase in volume comes with substantial costs. A recent study by the European Union estimated the total cost of spam worldwide is over $8 billion in connection time alone.[4] Domestically, up to $3 of a consumer's monthly ISP bill goes towards paying for spam.[5] These costs can be traced to the time it takes to open, review, and delete spam, the increased network capacity necessary to process it, and the displacement of bandwidth and time that otherwise would be used for normal email and work.

The Federal Trade Commission

Spam is legal. Recognizing this fact, and acting within its limited jurisdiction, the FTC only goes after fraudulent spam, bringing more than 30 enforcement actions against purveyors of false and misleading email communications in recent years.[6] One of the FTC's initial targets was spam chain-letter schemes. During one of these investigations, FTC v. Boivin, the FTC uncovered a deceptive email that promised "$46,000 or more in the next 90 days" to recipients who sent in five dollars cash to each of four participants listed at the top of an attached list. Skeptical recipients were told to contact the FTC's Associate Director for Marketing Practices to ensure its legality. In the press release announcing the settlement with these spammers, Eileen Harrington, the Associate Director referred to in the email, replied "I am the Associate Director for Marketing Practices, and these chain letters are illegal." [7]

Timothy J. Muris, Chairman of the FTC, also recently announced stepped-up enforcement efforts regarding false and misleading spam, particularly deceptive claims that a consumer can remove themselves from a mailing list when no steps are taken by the marketer to effect such a removal.[8] As part of this initiative, the FTC, along with six state agencies and the Canadian Competition Bureau, has sent more than 75 letters warning spammers that deceptive "unsubscribe" claims in spam are illegal.[9] Howard Beales, the FTC's Director of the Bureau of Consumer Protection, has stated that these enforcement actions are the beginning of a "systematic attack" on fraudulent and deceptive spam and opt-out notices.[10]

The FTC has also implemented a number of consumer education programs related to unsolicited email[11] and provided guidance to businesses who use email marketing campaigns.[12] In addition, the FTC has developed a widely utilized monitoring system that allows private entities and law enforcement agencies to forward UCE to an FTC mailbox, dubbed the "Refrigerator," where it is indexed and maintained.[13] The UCE collected is often used to strengthen Commission enforcement actions, including recent actions against distributors of deceptive chain emails and companies using spam to sell worthless domain names, or as part of consumer or business education programs. Since January 1998, over 8.3 million UCEs have been sent to the Refrigerator.

The Senate has voted S. 630, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001 ("CAN SPAM Act") out of committee.

In the House, the bills receiving the most attention have been H.R. 718 and H.R. 1017 (both referred to the as the Anti-Spamming Act of 2001) and H.R. 113 (Wireless Telephone Spam Protection Act). H.R. 113 and 1017 are both sitting in Committee, and H.R. 718 was sent to the floor and placed on the union calendar last year, with no action yet. It is unlikely that passage will occur this year.

While the FTC's efforts have been successful, spam is difficult to contain. In response, the FTC continues to step up its efforts, devoting substantial resources to detect and eliminate new types of deceptive spam schemes. Specifically, the FTC has targeted email with misleading or deceptive subject lines and sellers of bulk lists of consumer email addresses.[14] The Commission's enforcement actions in this area are tied closely to its agenda.[15]

Pending Legislation

Constitutional considerations have deterred passage of comprehensive spam legislation. Proponents of unsolicited email have argued that spam is protected free speech. However, with the ever-increasing amount of resources devoted to receiving, reading, and deleting spam, as well as the amount of illegal spam being distributed, consumers have begun to complain. And when consumers, who are also constituents, begin to complain, legislators take note.

The "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001" (S. 630), also known as the "CAN SPAM Act of 2001," seeks to control the costs of UCE, while strengthening consumers' ability to choose whether or not to receive UCE. Senator Conrad Burns, sponsor of S. 630, has stated that this bill is designed to "strangle out spam email by imposing steep fines and empowering consumers with the choice to close their doors to hyper-marketing once and for all."[16]

The "Can Spam Act" would require all UCE to disclose that an unsolicited email is an advertisement in header or subject lines, and to include an opt-out notice, a valid return email address for the sender, and a valid postal address for the sender. The bill also would make it unlawful to send emails with false or misleading subject lines. Enforcement actions could be initiated by various federal agencies, including the FTC, and state attorneys general.[17] ISPs would be permitted to bring private causes of action to keep UCE off of their networks and state attorneys general would have the ability to bring suit on behalf of private citizens. S. 630 would not create, however, a private right of action for consumers. During Committee hearings on an early version of the bill, Jerry Cerasale of the Direct Marketing Association stated, "a consumer cause of action would create a very substantial bounty for class action lawyers that would produce very substantial damage awards wholly unrelated to the costs imposed by UCE."[18]

The bill would further strengthen the FTC's enforcement authority by allowing fines of up to $10 per violating email with a limit of $500,000, an amount that could triple for a willful violation. Finally, S. 630 subjects spammers who intentionally disguise their identities to misdemeanor criminal penalties.

There has been some opposition to S. 630 by advocacy groups, who favor a private right of action for consumers not found in S. 630, question the enforcement provisions of the bill, and prefer an "opt-in" versus "opt-out" requirement. Some of these groups also argue that the Can Spam Act, and similar bills, would unfairly restrict email marketing and put electronic commerce at a disadvantage. In addition, some groups have expressed concern that S. 630 would set a higher deceptive trade practice standard for spam than exists for other types of commercial activity under the FTC Act.[19] Despite its critics, S. 630 was approved and sent to the floor by the Senate Commerce Committee on May 17, 2002. In light of accounting scandals and homeland security issues, S.630 is not likely to come to a vote in the Senate this year. But momentum is building for serious consideration of a spam bill in the 108th Congress.

While there have been a number of bills introduced in the House, three bills have received the most attention: H.R. 718 and H.R. 1017 (both referred to the as the Anti-Spamming Act of 2001) and H.R. 113 (Wireless Telephone Spam Protection Act).

Representative Heather Wilson introduced H.R. 718, a bill that would prohibit false headers in UCE and would require labels on sexually oriented commercial email messages. This bill, like most others, would seek to direct the costs of spam back to the spammers through various penalty provisions. Representative Dingell, in support of H.R. 718, stated, "it is simply unfair to require the taxpaying public to foot the bill for the damage caused by spammers."[20]

Representative Bob Goodlatte introduced H.R. 1017, which would criminalize the intentional transmission of UCE with knowledge that such message falsifies an Internet domain or other identifier. The bill would also make it illegal to sell or distribute computer programs designed to conceal the source of the UCE.

H.R. 113, introduced by Representative Rush Holt, would prohibit the use of text, graphic, or image messaging systems of wireless telephone systems to transmit unsolicited commercial messages.

There has been little action in the House on any of these bills as of late. H.R. 113 and 1017 are both sitting in Committee, and H.R. 718 was sent to the floor and placed on the union calendar last year, with no action yet. It is unlikely that passage will occur this year.

(Endnotes)

1 Statement of Esther Dyson, author, Internet commentator, and President, EDventure Holdings, www.brightmail.com/external_cache/Whamming_the_spammers_.shtml.

2 http://www.businessweek.com/technology/content/mar2002/tc2002031_8613.htm.

3 Jenna Greene, Two Bills Seek to Provide Protection Against Email Spam, New York Law Journal at 5 (May 17, 2001).

4 http://europa.eu.int/comm/internal_market/en/dataprot/studies/spam.htm.

5 http://www.infoworld.com/articles/en/xml/00/01/10/000110enspam.xml.

6 *See, e.g. FTC v. Paul K. Boivin* (M. D. Fla. filed Jan. 14, 2002). In Boivin, the FTC settled charges with seven defendants who had been allegedly spamming consumers with deceptive electronic chain letters. Other recent FTC enforcement actions involving deceptive spam include *FTC v. Linda Jean Lightfoot*, No. C-3-02-145 (S. D. Oh. filed Mar. 29, 2002); *FTC v. John Lutheran* (S. D. Cal. filed Jan. 14, 2002); *FTC v. Fernando Pacheco*, (D. R.I. filed Jan. 14, 2002).

7 Statement of Eileen Harrington, Associate Director of Marketing Practices, FTC Pres Release, Feb. 12, 2002.

8 Remarks of FTC Chairman Timothy J. Murris, http://www.ftc.gov/speeches/muris/gmason.htm.

9 http://www.ftc.gov/opa/2002/04/spam.htm.

10 http://www.businessweek.com/bwdaily/dnflash/feb2002/nf20020221_7724.htm. Dr. Beales has also stated that deceptive "unsubscribe" spam results in increased spam for consumers, which leads to increased costs. See, Remarks of Howard Beales, The FTC's Consumer Protection Agenda: Continuity and Change, The Promotional Marketing Association Annual Meeting (Dec. 5, 2001).

11 Trouble @ the In-Box ; Spam's Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email.

12 On January 30, 2001, the FTC and the Electronic Retailing Association hosted an online marketing seminar for retailers, marketers, and suppliers.

13 uce@ftc.gov.

14 http://www.internetnews.com/IAR/article.php/12_1142711.

15 *See* Remarks of Howard Beales, The FTC's Consumer Protection Agenda: Continuity and Change, The Promotional Marketing Association Annual Meeting (Dec. 5, 2001).

16 http://burns.senate.gov/p020517a.htm.

17 S. 630 would provide enforcement powers to the FTC, pursuant to the FTC Act, and certain other federal agencies pursuant to various statutes, including the Securities and Exchange Commission, the Board of the National Credit Union Administration, the Secretary of Transportation, the Secretary of Agriculture, and the Federal Communications Commission.

18 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001: Hearings on S. 630 Before the Senate Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation, 106th Congress (2001) (state-

ment of Jerry Cerasale, The Direct Marketing Association, Inc.)

19 http://www.ecomforum.org/junkemail.html.

20 H.R. Rep. No. 107-41, pt. 1 (2001).

Privacy Regulation

Summer 2002

Consumer Protection Committee

Robert M. Langer
Chair
Wiggin & Dana LLP
Hartford, CT
rlanger@wiggin.com

Julie Brill
Vice-Chair
Office of the Attorney General
of the State of Vermont
Montpelier, VT
jbrill@atg.state.vt.us

Lesley A. Fair
Vice-Chair
Federal Trade Commission
Washington, DC
lfair@ftc.gov

August Horvath
Vice-Chair
Weil, Gotshal & Manges LLP
New York, NY
august.horvath@weil.com

John Villafranco
Vice-Chair
Collier Shannon Scott PLLC
Washington, DC
jvillafranco@colliershannon.com

Computer and Internet Committee

David H. Evans
Co-Chair
Jones, Day, Reavis & Pogue
Washington, DC
dhevans@jonesday.com

Leslie C. Overton
Co-Chair
Gray, Cary, Ware & Freidenrich LLP
Sacramento, CA
loverton@graycary.com

Mark C. Del Bianco
Vice-Chair
Skadden, Arps, Slate, Meagher & Flom LLP
Washington, DC
mdelbian@skadden.com

Patrick Kelleher
Vice-Chair
Gardner Carton & Douglas
Chicago, IL
pkelleher@gcd.com

Gail Levine
Vice-Chair
Federal Trade Commission
Washington, DC
glevine@ftc.gov

Paul Saint-Antoine
Vice-Chair
Drinker, Biddle & Reath LLP
Philadelphia, PA
paul.saint-antoine@dbr.com