

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
“UNSOLICITED COMMERCIAL EMAIL”

Before the

SUBCOMMITTEE ON
COMMUNICATIONS

of the

COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION,
U.S. SENATE

Washington, D.C.

April 26, 2001

Mr. Chairman, I am Eileen Harrington of the Federal Trade Commission's Bureau of Consumer Protection. The Federal Trade Commission is pleased to provide testimony today on the subject of unsolicited commercial email, the consumer protection issues raised by its widespread use, the FTC's program to combat deceptive and fraudulent unsolicited commercial email, and the FTC's views on the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001" (S. 630), which Chairman Burns has proposed.¹

I. Introduction and Background

A. FTC Law Enforcement Authority

As the federal government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by taking action against unfair or deceptive acts or practices, and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.² The Commission's

¹ The views expressed in this statement represent the views of the Commission. My responses to any questions you may have are my own.

² 15 U.S.C. § 45(a). The Commission also has responsibilities under more than 45 additional statutes, *e.g.*, the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.*, which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the

(continued...)

responsibilities are far-reaching. With certain exceptions, this statute provides the Commission with broad law enforcement authority over virtually every sector of our economy.³ Commerce on the Internet, including unsolicited commercial electronic mail, falls within the scope of this statutory mandate.

B. Concerns about Unsolicited Commercial Email

Unsolicited commercial email -- “UCE,” or “spam,” in the online vernacular -- is any commercial electronic mail message sent, often in bulk, to a consumer without the consumer’s prior request or consent. The very low cost of sending UCE differentiates it from other forms of unsolicited marketing, such as direct mail or out-bound telemarketing. Those marketing techniques, unlike UCE, impose costs on senders that may serve to limit their use.

Generally, well-known manufacturers and sellers of consumer goods and services do not send UCE. Rather, such merchants use *solicited* email to give consumers information that they have requested about available products, services, and sales. For example, consumers may agree in advance to receive information about newly-published books on subjects of interest, online catalogues for products or services frequently purchased, or weekly emails about discounted airfares.

²(...continued)

Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

³The FTC has limited or no jurisdiction over specified types of entities and activities. These include banks, savings associations, and federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. *See, e.g.*, 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. §§ 1011 *et seq.* (McCarran-Ferguson Act).

These examples of bulk commercial email sent at the consumer's request demonstrate the value of consumer sovereignty to the growth of Internet commerce. Giving consumers the ability to *choose* the information they receive over the Internet -- known in the industry now as "permission-based" marketing -- seems likely to create more confidence in its content and in the sender.

By no means is all UCE is fraudulent, but fraud operators, who are often among the first to exploit any technological innovation, have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE. Not only are fraud operators able to reach millions of individuals with one message, but they can misuse the technology to conceal their identity. Many spam messages contain false information about the sender and where the message was routed from, making it nearly impossible to trace the UCE back to the actual sender. In the same vein, UCE messages also often contain misleading subject lines and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes.

Bulk UCE burdens (indeed, sometimes cripples) Internet service providers and frustrates their customers. The FTC's main concern with UCE, however, is its widespread use to disseminate false and misleading claims about products and services. The Commission believes the proliferation of deceptive bulk UCE on the Internet poses a threat to consumer confidence in online commerce and thus views the problem of deception as a significant issue in the debate over UCE.

II. The Federal Trade Commission's Approach to Fraud on the Internet

In 1994, the Commission filed its first enforcement action against deception on the Internet, making it the first federal enforcement agency to take such an action.⁴ Since that time, the Commission has brought 173 law enforcement actions against more than 575 defendants to halt online deception and fraud. The pace of our Internet law enforcement has been increasing, in step with the growth of commerce -- and fraud -- on the Internet; over two-thirds of the FTC's Internet-related actions have been filed since the beginning of 1999.

The Commission brings to the Internet a long history of promoting competition and protecting consumers in other once-new marketing media. Recent innovations have included 900-number technology and telemarketing. The development of each of these advances in the marketplace was characterized by early attempts of fraud artists who sought to capitalize on the new way of doing business. In each instance, the Commission used its statutory authority under Section 5 of the FTC Act to bring tough law enforcement actions to halt specific deceptive or unfair practices, and establish principles for non-deceptive marketing.⁵ In some instances, most notably national advertising, industry

⁴ *FTC v. Corzine*, CIV-S-94-1446 (E.D. Cal. filed Sept. 12, 1994).

⁵Section 5 of the FTC Act, 15 U.S.C. § 45, authorizes the Commission to prohibit unfair or deceptive acts or practices in commerce. The Commission may initiate administrative litigation, which may culminate in the issuance of a cease and desist order. It can also enforce Section 5 and other laws within its mandate by filing actions in United States District Courts under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), seeking injunctions, consumer redress, disgorgement, and other equitable relief. Section 18 of the FTC Act, 15 U.S.C. § 57a, authorizes the Commission to promulgate trade regulation rules to prohibit deceptive or unfair practices that are prevalent in specific industries. Courts may impose civil penalties of up to \$11,000 per violation of Commission trade regulation rules.

took an aggressive and strong self-regulatory stance that resulted in dramatic improvements in advertising and marketing practices.⁶

In other instances, at the direction of Congress or on its own initiative, the Commission has issued trade regulation rules to establish a bright line between legitimate and deceptive conduct.⁷

III. The Commission's Approach to Unsolicited Commercial Email

A. Monitoring the Problem

The Federal Trade Commission closely monitors the development of commerce on the Internet. Since the inception of the Internet as a commercial medium, the Commission has conducted a series of hearings and public workshops so that it could have the benefit of views from a wide range of stakeholders.⁸ In June 1997, at a workshop devoted to issues of privacy on the Internet, the Commission heard discussion of three distinct UCE problems: (1) deception in UCE content; (2) economic and technological burdens on the Internet and delivery networks caused by the large volume

⁶For example, the National Advertising Division of the Council of Better Business Bureaus, Inc., operates the advertising industry's self-regulatory mechanism.

⁷For example, the Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations (the "Cooling-Off Rule"), 16 C.F.R. Part 429; the Mail or Telephone Order Merchandise Rule, 16 C.F.R. Part 435; the Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act of 1992 ("The 900-Number Rule"), 16 C.F.R. Part 308; and the Telemarketing Sales Rule Pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 16 C.F.R. Part 310.

⁸The first of these was held in the fall of 1995, when the Commission held four days of hearings to explore the effect of new technologies on consumers in the global marketplace. Those hearings produced a staff report, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

of UCE being sent; and (3) costs and frustrations imposed on consumers by their receipt of large amounts of UCE.

While the Commission has maintained a focus on deception perpetuated through UCE, industry and advocacy groups that participated in the privacy workshop directed their attention to the economic and technological burdens caused by UCE. Under the leadership of the Center for Democracy in Technology, these groups spent a year studying the problem and identifying possible solutions, and in July 1998 issued their “Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail.”⁹ This report recommended the pursuit of technologies and public policies that would provide consumers with more control over the UCE they receive. Specifically, the report:

- urged marketers to give consumers a choice to “opt in” or “opt out” of receiving a UCE solicitation; and
- urged law enforcement to continue to attack fraudulent UCE solicitations, including those with deceptive “header” information.¹⁰

On another front, in 1998 the FTC set up a special electronic mailbox reserved for UCE in order to assess, first hand, emerging trends and developments. With the assistance of Internet service providers, privacy advocates, and other law enforcers, staff publicized the Commission’s UCE mailbox, “uce@ftc.gov,” and invited consumers and Internet service providers to forward their UCE to it. The

⁹This report is available at www.cdt.org/spam.

¹⁰“Header” information, at minimum, includes the names, addresses, or descriptions found in the “TO:”, “FROM:”, and “SUBJECT:” lines of an email. It also includes the technical description of the route an email has traveled over the Internet between the sender and recipient.

Commission also created a database in which all of the forwarded UCE messages are stored. Over 8,300,000 pieces of UCE have been forwarded to the Commission since January 1998, and the UCE mailbox receives an average of 10,000 new pieces of UCE every day, seven days a week. UCE received and entered in the database within the preceding six months is searchable. Periodically, staff has used the data to supplement law enforcement and consumer and business education efforts. Commission staff has recently made arrangements to purchase new indexing software that will allow staff to conduct much more sophisticated searches as well as manipulate the data to determine trends and patterns in the UCE received.

B. Aggressive Law Enforcement

The Commission has responded to fraudulent UCE with a vigorous law enforcement program. To date, about 30 of the Commission's Internet cases have targeted scams in which spam was an essential, integral element. Most of these cases have been Section 13(b) actions in federal district court. For example, in May 1999, the Commission filed *FTC v. Benoit*.¹¹ This scheme used the ruse of a spam notification about charges purportedly to be billed to consumers' credit card accounts to lure the consumers into calling an expensive international telephone number.¹² The initial spam message

¹¹*FTC v. Benoit*, No. 3:99 CV 181 (W.D.N.C. filed May 11, 1999). This case was originally filed under the caption *FTC v. One or More Unknown Parties Deceiving Consumers into Calling an International Audiotext Service Accessed Though Telephone Number (767) 445-1775*. Through expedited discovery, the FTC learned the identities of the perpetrators of the alleged scam by following the money trail connected to the telephone number. Accordingly, the FTC amended its complaint to specify the defendants' names.

¹²A similar scheme that used spam was targeted in *FTC v. Lubell*, No. 3-96-CV-80200 (S.D. Ia. 1996). In that case, the spam urged consumers to call an expensive international number to hear a message that purportedly would inform them about discount airline tickets and how to enter a sweepstakes.

purported to inform consumers that their “orders had been received and processed” and that their credit card accounts would be billed for charges ranging from \$250 to \$899. In fact, the consumers had not ordered anything. The spam advised recipients to call a specified telephone number in area code 767 with any questions about the “order” or to speak to a “representative.” Many consumers were unaware that area code 767 is in a foreign country -- Dominica, West Indies. But because Dominica is included within the North American Numbering Plan,¹³ it was not necessary to dial 011 or any country code to make the calls.

Consumers who called to prevent charges to their credit cards, expecting to speak to a “representative” about the erroneous “order,” were connected to an adult entertainment “audiotext” service.¹⁴ Later, these consumers received charges on their monthly telephone bills for the international long-distance call to Dominica, West Indies. The defendants shared in the revenue received by a foreign telephone company for the costly international calls. The defendants hid their tracks by using forged headers in the spam they used to make initial contact with consumers.

The final stipulated order that resolved this case includes a provision specifically prohibiting the defendants from sending or causing to be sent any email (including unsolicited commercial email) that misrepresents the identity of the sender of the email or the subject of the email. The Order thus bans the defendants from falsifying information in the “from” and “subject” lines of emails, as well as in the text of the message.

¹³See <http://www.nanpa.com/home>.

¹⁴The term “audiotext services” describes audio information and entertainment services offered over the telephone through any dialing pattern, including services accessed via 900-number, as well as international and other non-900-number, dialing patterns.

Another recent case, *FTC v. Martinelli*,¹⁵ targeted an alleged pyramid scheme that centered on spam. The defendants in that case ran an operation called DP Marketing, which was a Connecticut-based pyramid scheme, elaborately disguised as a work-at-home opportunity. DP Marketing solicited new recruits through “spam” and through newspaper classified ads across the country. The spam contained messages such as: “National Marketing Company seeks individuals to handle office duties from home. This is a full or part-time position with a salary of \$13.50/hr. The position consists of processing applications for credit, loans or employment, as well as online consumer service.”

Consumers who responded by visiting DP Marketing's Web site or by calling the company received a pitch stating that they could receive \$13.50 per hour by just processing orders for the company from the comfort of their own homes. The defendants also represented that no experience was necessary, and that for a “registration fee” ranging from \$9.95 to \$28.72 purchasers would be sent everything needed to get started, including telephone scripts, product sheets, time sheets and ID numbers. What consumers actually got was a kit instructing them first to place advertisements identical to the ones to which they had responded, and then to read the same script to people who responded to their ads. Instead of \$13.50 per hour, consumers’ earnings depended on the number of new victims they recruited.

¹⁵*FTC v. Martinelli*, No. 399 CV 1272 (CFD) (D. Conn. filed July 7, 1999). Other alleged pyramid schemes that utilized spam have been targets of FTC enforcement action. *See, e.g., FTC v. Nia Cano*, No. 97-7947-IH-(AJWx) (C.D. Cal. filed Oct. 29, 1997); *In re: Calvin P. Schmidt*, Docket No. C-3834 (final consent Nov. 16, 1998).

The FTC complaint alleged that the defendants misrepresented to consumers that DP Marketing offers jobs at a specified salary; failed to disclose the material fact that they were offering a pyramid work-at-home scheme; and provided to others the “means and instrumentalities” to commit unlawful and deceptive acts. On November 14, 2000, the court entered a stipulated final order banning the defendants from future pyramiding, barring them from misrepresenting the availability and profitability of jobs, and requiring the defendants to pay \$72,000 in consumer redress.

The Commission has also brought a number of cases against credit repair scams that used spam as an integral aspect of their deception.¹⁶ In a particularly pernicious variation on this scheme, consumers are urged to create a new credit identity in order to fix their credit. Using spam messages such as “BRAND NEW CREDIT FILE IN 30 DAYS,” these scammers induce consumers to purchase instructions about how one can obtain a federally-issued, employee or taxpayer identification number, and use these numbers illegally in place of social security numbers to build a new credit profile that will purportedly allow one to get credit that would be denied based on one’s true credit history. In fact, using a false identification number to apply for credit is a felony – a point these scammers omit from their solicitations. The Commission, either on its own or through the Department of Justice, filed cases against seven operations that used this type of deceptive spam.¹⁷

¹⁶*FTC v. Consumer Credit Advocates*, No. 96 Civ. 1990 (S.D.N.Y. filed Mar. 19, 1996); *FTC v. Dixie Cooley, d/b/a DWC*, No. CIV-98-0373-PHX-RGS (D. Ariz. filed March 4, 1998).

¹⁷*FTC v. Cliff Cross and d/b/a Build-It-Fast*, Civ. No. M099CA018 (W.D. Tex. filed Feb. 1, 1999); *FTC v. Ralph Lewis Mitchell, Jr.*, No. CV 99-984 TJH (BQRx) (C.D. Cal. filed Jan. 29, 1999); *FTC v. Frank Muniz*, No. 4:99-CV-34-RD (N.D. Fla. filed Feb. 1, 1999); *U.S. v. A. James Black*, No. 99-113 (M.D. Fla. filed Feb. 2, 1999); *FTC v. James Fite, d/b/a Internet Publications*, No. CV 99-04706JSL (BQRx) (C.D. Cal. filed April 30, 1999); *U.S. v. David Story, d/b/a Network Publications*, 3-99CV0968-L (N.D. Tex. filed April 29, 1999); and *FTC v. West Coast Publications, LLC.*, CV 99-

(continued...)

More recently, in *FTC v. Para-Link International*,¹⁸ the FTC sued several Florida-based companies that were using spam to market a work-at-home paralegal business opportunity. The Commission's complaint charged that the defendants use spam to induce consumers to purchase the business opportunity for \$395-495. The spam contained representations such as: "Make Over \$200 An Hour," and "You Can Process Simple Divorces and Bankruptcies From Home and Make Over \$200 An Hour in as little as 30 Days!!!"; and urged prospective purchasers to call a toll-free number for more information. Defendants promised that the business opportunity would include training so purchasers could become at-home paralegals; defendants also promised to refer a steady stream of clients to purchasers of the business opportunity for a fee of \$25 each.

According to the FTC's complaint, few consumers who purchased the business opportunity from the defendants ever realized these earnings. The court entered a temporary restraining order ("TRO") against the defendants on October 17, 2000, ordering them to cease operations, freezing their assets, and appointing a receiver to take charge of the companies. Subsequently, the court issued an order that extended the relief granted in the TRO pending issuance of a preliminary injunction.

¹⁷(...continued)
04705GHK (RZx) (C.D. Cal. filed April 30, 1999).

¹⁸*FTC v. Para-Link International*, No. 8:00-CV-2114-T-27E (M.D. Fla. filed Oct. 16, 2000).

Other types of deceptive schemes that use UCE have also been targets of FTC enforcement action, such as deceptive business opportunities¹⁹ and deceptive weight loss schemes.²⁰ As these cases illustrate, the Commission's focus has been on the deceptive content of UCE messages.

C. *Comprehensive Consumer and Business Education*

The Commission has published nine consumer publications related to UCE, available in paper format and downloadable from the FTC's Web site. More than 1.6 million of these documents have been distributed to consumers, either through paper copies or via access to the Commission's Web site.²¹

The first, *Phone, Email and Pager Messages May Signal Costly Scams*, was published in 1996. It has been distributed in paper form over 16,000 times and has been accessed at the FTC's Web site more than 18,000 times. Two versions of the related *Trouble @ the In-Box* help consumers identify some of the scams showing up in electronic in-boxes and offer tips and suggestions for assessing whether an opportunity is legitimate or fraudulent. These publications also advise consumers about how to handle UCE and offer ideas for consumers to control the flow of UCE. The publications steer consumers to additional resource materials that can help them determine the validity of a promotion or money making venture. To date, over 87,000 paper copies of the brochures have been distributed, and they have been accessed on the FTC's Web site nearly 53,000 times.

¹⁹ *FTC v. Internet Business Broadcasting, Inc.*, No. WMN-98-495 (D. Md. filed Feb. 19, 1998); *United States v. PVI, Inc.*, No. 98-6935 (S.D. Fla. filed Sept. 1, 1998).

²⁰ *TrendMark International, Inc.*, Docket No. C-3829 (final consent Oct. 6, 1998)

²¹ The distribution and access numbers for these consumer education materials are accurate as of March 31, 2001.

How to Be Web Ready is a reader's bookmark that offers consumers tips for safe Internet browsing. It provides guidance for consumers on how to safeguard personal information, question unsolicited product or performance claims, exercise caution when giving their email address, guard the security of financial transactions, and protect themselves from programs and files that could destroy their hard drives. A number of corporations and organizations have provided a link from their Web sites to the tips on the FTC's Web site, including Circuit City, Borders Group Inc., Netcom, Micron, and Compaq. More than 94,000 paper copies of the bookmark have been distributed, and it has been accessed more than 31,000 times on the FTC's Web site. A related publication, *Site-Seeing on the Internet: A Consumer's Guide to Travel in Cyberspace*, with similar helpful hints, has been accessed nearly a million times on the FTC's Web site, and over 165,000 papers copies have been distributed.

In July 1998, the FTC launched a public education campaign called *Spam's Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email* to publicize the most prevalent UCE scams. The list of scams was culled from a sampling of more than 250,000 spam messages that consumers had forwarded to the FTC's spam mailbox at uce@ftc.gov. The consumer alert identified the following twelve types of deceptive solicitations and described how each operates: business opportunity schemes; bulk email programs²²; chain letters; work-at-home schemes; health and diet scams; effortless income; free goods; investment opportunities; cable descrambler kits; guaranteed loans or credit on

²²These schemes claim that one can make money sending one's own solicitations via bulk e-mail. They offer to sell one lists of e-mail addresses or software to allow one to make the mailings. What they don't mention is that the lists are of poor quality and that sending bulk email violates the terms of service of most providers of Internet access service.

easy terms; credit repair; and vacation prize promotions. More than 24,000 paper copies of this consumer alert have been distributed, and it has been accessed more than 100,000 times on the FTC's Web site.

In March 2000, the Commission published an alert titled *Unsolicited Mail, Telemarketing and Email: Where to Go to "Just Say No"* which provided information to consumers on how to control junk mail and email. Over 21,000 copies of this alert have been distributed in paper form, and it has been accessed over 20,000 times on the FTC's Web site. In September 2000, the Commission published a consumer alert entitled *The Lowdown on Chain Letters* in an effort to warn consumers about the risks of chain letters that arrive via email. Over 10,000 paper copies of this brochure have been distributed, and it has been accessed over 8,200 times on the FTC's Web site.

In January of this year, the FTC published *Cracking Down on Mail, Email and Fax Scams: Project Mailbox* that offers tips to consumers about avoiding being scammed by mail or email offers. The publication is only available on the FTC's Web site, and has been accessed online nearly 1,300 times to date.

IV. The Commission's Views on S. 630, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001" (the "CAN SPAM Act of 2001").

The Commission generally favors the underlying goals of S. 630, which are to help control the additional costs and other potential negative effects that UCE can impose on Internet access service providers and other businesses and consumers that use the Internet, and to support consumer choice in the matter of whether to receive UCE. There are two basic problems that

S. 630 addresses. First, there is the problem of fraudulent or deceptive UCE, and second, but also important, is the infrastructure problem that flows from the sheer volume of UCE. UCE, even if not deceptive, may lead to significant disruptions and inefficiencies in Internet services, and may constitute a great nuisance to consumers and businesses using the Internet. Both of these problems together pose a threat to consumers' confidence in the Internet as a medium for personal electronic commerce.²³

S. 630 mandates the "permission-based" marketing model already adopted by many well-known manufacturers and sellers of consumer goods and services, and advocated by the Center for Democracy in Technology and other groups in their 1998 "Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail."

Section 5 of S. 630 would make it unlawful to initiate transmission of a commercial email message that does not contain specified items of information designed to enable consumers to identify UCE and to prevent future receipt of it from that sender. These disclosures, required to be clear and conspicuous, are: an identification that the email is an advertisement or solicitation; a notice of the opportunity (mandated by the Bill) to decline to receive further UCE from the sender to the recipient; a functioning return email address to which a recipient may send a reply to the sender to indicate a desire

²³See *Unsolicited Commercial Email: Hearing Before the Subcomm. on Telecomm., Trade and Consumer Protection of the House Comm. on Commerce*, 106th Cong. (Nov. 1999) (statements of various providers of internet access service detailing costs and loss of goodwill caused by UCE); Serge Gauthronet & Etienne Drouard, *Unsolicited Commercial Communications and Data Protection* (Jan. 2001), p. 9. (finding, in this study undertaken by the Commission of European Communities, that the global cost to Internet users may be conservatively estimated at i 10 billion (\$8.943 billion) annually); See generally the 1998 *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail* (citing several types of costs imposed on consumers and businesses by UCE – intrusion on consumers' privacy, lost opportunity costs, Internet infrastructure costs, access and storage fees, and reputational harms) (available at www.cdt.org/spam).

not to receive further emails from that sender; and a valid physical postal address of the sender.

Section 5 of S. 630 would also make it unlawful:

- for a sender, or any person acting on behalf of the sender, to initiate the transmission of UCE to any recipient after that recipient has sent to the email address provided by the sender a request not to receive further email from that sender;
- for any person to initiate the transmission of a commercial email message that “contains, or is accompanied by, header information that is materially or intentionally false or misleading, or not legitimately obtained;” or
- for any person to initiate the transmission of a commercial email message “with a subject heading that such person knows is likely to mislead the recipient about a material fact regarding the contents or subject matter of the message.”

S. 630 includes a multi-faceted enforcement scheme. First, Section 5 of the Bill, described above, would be enforceable by the FTC, and any violation of it would be treated as if it were a violation of an FTC Trade Regulation Rule adopted pursuant to Section 18 of the FTC Act, 45 U.S.C. § 57a. This means that each such violation would subject the violator to a maximum civil penalty of \$11,000 in an enforcement action by the FTC.²⁴

²⁴An action seeking civil penalties for violation of a Trade Regulation Rule promulgated under Section 18 must be forwarded by the Commission to the Department of Justice for filing and litigating. If the Department of Justice declines to file the complaint within 45 days, the Commission, through its own attorneys, may file and litigate the matter. 45 U.S.C. § 56(a). Pursuant to Section 13(b) of the FTC Act, (continued...)

Second, the Bill would allow other federal agencies that have jurisdiction over industries whose activities are wholly or partially exempt from the FTC's jurisdiction, such as banking and common carriers, to enforce the Bill. Third, both providers of Internet access service and the Attorneys General of the various states would have enforcement authority to obtain injunctions against violations of Section 5 of the Bill, and to recover damages.²⁵

In addition to civil enforcement of Section 5 of S. 630, Section 4 of the Bill would establish liability for criminal fines or up to one year imprisonment for anyone who "intentionally initiates the transmission of any unsolicited commercial electronic mail message . . . with knowledge that such message contains or is accompanied by header information that is materially or intentionally false or misleading."

S. 630 specifically provides that it would have no effect on the ability of providers of Internet access service to enforce their anti-UCE policies. Finally, the Bill would mandate a study by the Commission within 18 months that would provide a detailed analysis of the effectiveness and enforcement of the Bill's provisions.

²⁴(...continued)

45 U.S.C. § 53(b), however, the Commission may file and litigate, through its own attorneys, any action seeking injunctive relief, consumer restitution, disgorgement of ill-gotten gains or other equitable remedies without first forwarding the matter to the Department of Justice.

²⁵Successful plaintiff States or providers of Internet access service could recover an amount equal to actual damages or statutory damages of up to \$10 for each separately addressed unlawful message received by the states' residents, with a maximum of \$500,000, and in cases of willful and knowing violations, three times this amount. Recovery of costs and reasonable attorneys' fees would be authorized. Section 6(e) of S. 630 would establish an affirmative defense in cases brought by providers of Internet access service or the States where a defendant can show that it has established and implemented compliance policies and procedures, and that any violation occurred despite good faith efforts to follow those policies and procedures.

The Commission's views, set forth below, on the provisions of S. 630, are informed by workshops and other discussions the Commission has had with interested members of the Internet and marketing industry, as well as the Commission's law enforcement experience in the area of UCE, and in related areas, such as the "Do Not Call" provision of the Telemarketing and Consumer Fraud and Abuse Prevention Act.²⁶ Where useful, the Commission also sets forth its views on H.R. 718, another legislative proposal dealing with UCE that is similar to S. 630.²⁷

A. *The Definition of the Term "Commercial Electronic Mail Message" [§ 3(2) of S. 630].*

A key term used throughout S. 630 is "commercial electronic mail message"; this term is defined in Section 3 of the Bill. The relevant portion of the definition provides that "an electronic mail message shall not be considered to be a commercial electronic mail message solely because such message includes . . . a reference or link to an Internet web site operated for a commercial purpose." Commission staff has observed that much UCE -- particularly UCE related to pornographic web sites -- consists of nothing more than such a reference or link. The definition as currently drafted could potentially be exploited by senders of such UCE to evade the requirements of the Bill. As a practical matter, it may be difficult to demonstrate to a Court that an email consisting of nothing more than a URL and perhaps a statement such as "check this web site!" falls within the Bill's definition of "commercial electronic mail message" -- *i.e.*, that its "primary purpose . . . is to advertise or promote, for a commercial purpose, a commercial product or

²⁶5 U.S.C. § 6102(a)(3)(A).

²⁷This bill was introduced on January 3, 2001 by Rep. Heather Wilson, and is titled the "Unsolicited Commercial Electronic Mail Act of 2001."

service” – when the definition apparently demands more than a reference or link to an Internet web site operated for a commercial purpose to bring an email message within the scope of the Bill’s coverage. The House Bill currently under consideration, H.R. 718, avoids this problem by employing a definition of the term that tracks the definition in S. 630 but excludes the final problematic clause.

B. *The Prohibition Against Header Information That Is Materially or Intentionally False or Misleading, or Not Legitimately Obtained [§ 5(a)(1) of S. 630]*.

This provision would likely benefit consumers. Chief among consumer complaints about UCE is that consumers do not know who sent the UCE, and therefore do not know to whom they can send a request not to receive more UCE. In addition, false routing information can cause UCE messages to clog the email systems of providers of Internet access service, thereby slowing service to consumers trying to dial into the Internet through those providers of Internet access service or even completely shutting down the providers’ systems. Indeed, some providers have had to devote significant resources and staff to dealing with the sometimes overwhelming tide of UCE. These costs likely are passed on to consumers. The Commission is aware of no legitimate reason for using false header information.

The provision prohibiting falsification of routing information would allow a consumer to know who sent him or her the UCE. It could also help providers of Internet access service better handle the flow of both solicited and unsolicited commercial email, because valid routing information is more easily handled by the Internet access service providers’ email servers. This could result in fewer impairments to consumers’ Internet service, and possibly fewer costs passed on to consumers.

The provision strikes an appropriate balance by specifying that header information that is “materially . . . false or misleading” violates Section 5 of S. 630, while technically false header information

not meeting the standard of “materiality” would be actionable only if it could be shown that the falsehood was intentional. This appropriately ensures that inadvertent and relatively minor mistakes in header information will not trigger enforcement action or private lawsuits.

The language in the provision specifying that header information “not legitimately obtained” violates Section 5 of the Bill appears ambiguous. To ensure that this language does not create enforcement problems or engender unintended lawsuits, clarification would be helpful.

This provision would impose few if any additional costs on senders of commercial email. Further, the benefits to providers of Internet access service, recipients of email, and Internet users generally who desire and expect optimum convenience, likely outweigh any additional costs. Also, these provisions could make the use of commercial email a more effective marketing tool, because consumers likely would be more willing to trust the contents of a piece of UCE if they know the source of the email.

C. *The Prohibition Against a Subject Heading That Such Person Knows Is Likely to Mislead the Recipient about a Material Fact Regarding The Contents or Subject Matter of the Message [§ 5(a)(2) of S. 630].*

Consumers also complain about being misled by false subject lines of UCE. These misrepresentations lead them into believing that the contents are about one thing, but when they open the email, they discover that it is about something else entirely. For example, many senders of UCE that advertises pornography will use benign subject lines such as “Thanks for lunch” or “An old friend” that the average email recipient might believe are messages from someone he or she knows. In fact, to the consumer’s surprise, such UCE advertises pornographic Web sites. A subject line that non-deceptively described the contents of the UCE would allow a recipient to make an informed decision about whether to open the message.

The Commission is aware of no legitimate reason for using false subject heading information and supports this provision. Prohibiting deceptive subject lines would impose few, if any, additional costs on legitimate companies that use commercial email to promote their goods and services. Benefits to individual consumer recipients of email and to Internet users generally would outweigh any costs. As with the provisions discussed above, this provision could make the use of commercial email a more effective marketing tool, because consumers likely would be more willing to trust the contents of a piece of UCE if they could rely on representations made in the subject to accurately and truthfully reflect the message's contents.

This provision of S. 630, however, raises an issue about the Commission's authority to challenge deception under Section 5 of the FTC Act. Currently, the Commission could challenge a materially false or misleading subject line in a commercial email message under Section 5 of the FTC Act, as it could any other deceptive representation. The applicable legal standard that must be met to demonstrate a deceptive practice is that it is "likely to mislead consumers acting reasonably under the circumstances about a material fact."²⁸ S. 630 would establish a higher standard applicable to subject lines in commercial email messages by requiring a showing that the person who sent the email had knowledge that the subject line was likely to mislead the recipient about a material fact regarding the contents or subject matter of the message. The scienter requirement -- not an element of deception under Section 5 of the FTC Act -- would make it more difficult for the Commission to take action under S. 630 against materially false and misleading subject lines. As a matter of law enforcement, deceptive UCE should not be treated differently from any other deceptive act or practice. Moreover, the requirement of a showing that the subject line

²⁸*Cliffdale Associates, Inc.*, 103 F.T.C. 110, 165, *appeal dismissed sub nom., Koven v. F.T.C.*, No. 84-5337 (11th Cir. 1984).

was likely to mislead the *recipient*, and not a reasonable consumer, could increase the burden on the Commission in any action targeting materially false or deceptive representations made in subject lines of commercial email messages. This may require a showing that each individual recipient was likely to be misled, a very difficult burden to meet.

Because violating Section 5 of S. 630 would expose a person to liability for civil penalties of up to \$11,000 per violation, the Subcommittee may believe it appropriate to adopt stringent standards for liability in S. 630 to protect against penalties for what could be mere technical violations of the Bill.²⁹ However, the Commission believes that it would be useful for S. 630 to make clear that it does not affect the FTC's current ability to bring enforcement actions targeting materially false or deceptive representations in commercial email messages under Section 5 of FTC Act, pursuant to the criteria of, and seeking the remedies available under, that Act.³⁰ This could be accomplished by broadening the savings clause in Section 7(a) of the Bill.³¹ Therefore, clarification of an intent to leave intact the Commission's

²⁹It is noteworthy that Section 5(m)(1) of the FTC Act, 15 U.S.C. § 45(m)(1), requires the Commission, in actions to recover civil penalties for violations of trade regulation rules, to prove that the defendant violated the rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule." Moreover, this provision requires courts, in assessing civil penalties for rule violations, to "take into account the degree of [the defendant's] culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require."

³⁰In enforcement actions under Section 5 of the FTC Act the Commission can not seek civil penalties; instead it can seek administrative cease and desist orders, or, in the case of actions in district court under Sections 5 and 13(b) of the FTC Act, equitable remedies – injunctions, disgorgement, or restitution for consumer victims.

³¹In a related context, Congress ensured, in enacting the Telemarketing and Consumer Fraud and Abuse Prevention Act, that the Commission's ability to challenge deceptive telemarketing practices under the FTC Act would remain intact by including a broad savings clause: "Nothing contained in this chapter shall be construed to limit the authority of the Commission under any other provision of law." 15 U.S.C. § 6105(c):

powers under the FTC Act with respect to deceptive representations in subject lines of commercial email messages would be helpful.

D. The Requirement of an Email Address to Which Consumers Can Request to No Longer Receive UCE, and the Requirement That Senders of UCE Honor Such Requests [§§ 3 & 4 of S. 630].

These provisions would also likely benefit consumers. A major frustration among recipients of commercial email, and particularly with UCE, is that often any reply to the sender's email address "bounces back" and is never received by the sender. In such a case there is nothing the consumer can do to avoid receipt of additional commercial email from the same sender.

The provision requiring senders of commercial email messages to include a valid reply email address to which consumers may send requests to receive no more email, and requiring senders to honor such requests, would go a long way in helping consumers control the amount of commercial email, both solicited and unsolicited, they receive. However, it would likely impose some burdens on senders of commercial email. S. 630 would require every sender of commercial email to set up and maintain an email account to which consumers could send requests, and senders would have to monitor and update their mailing lists at least as often as every ten days. Nevertheless, the benefits of such a requirement would likely outweigh the costs to the senders.

E. The Requirement of an Identifier, Opt-out Opportunity, and Physical Address of the Sender in Each UCE Message.

S. 630 would require that every UCE message contain an identifier indicating that the message is an advertisement or solicitation. This provision would benefit consumers by enabling them to immediately recognize UCE messages as advertisements. It also may allow consumers to employ software that would filter UCE into a separate folder, or block UCE messages entirely. This provision would thus help

empower consumers to control the amount of UCE they receive. Notice that a message is an advertisement or solicitation would impose few, if any, additional costs on senders of UCE; they would merely have to add a few words (or even a few letters) to each message sent. Unlike print or broadcast communications, additional words in email messages do not add to their cost.

S. 630 would also require each UCE message to contain a clear and conspicuous notification of an opportunity for the recipient to decline to receive further UCE from the sender. This requirement would benefit consumers by helping them realize that they have a choice about whether they wish to receive additional UCE from a particular sender. Again, this requirement would impose few, if any, additional costs on senders of UCE; as with the identifier requirement, they would only have to add a few words to each message sent. It might also lower the overall volume of unwanted UCE on the Internet, thereby lowering certain cost burdens imposed on providers of Internet access service and potentially passed on to consumers.

Finally, S. 630 would require that each UCE message include the physical location of the sender. This provision might produce benefits in the form of enhanced consumer confidence in the legitimacy of senders. In cases where the UCE eventually leads to a transaction, the consumer would have an additional means of contacting the seller if the goods or services are not provided in accordance with the consumer's understanding, or, where applicable, if the consumer wishes to go to a seller's store. It is noteworthy that this provision of S. 630 is consistent with the guidelines of the Organization for Economic Co-operation and Development, which recommend that online businesses disclose their physical address. The Commission has endorsed those guidelines.³²

³²See, <http://www.ftc.gov/opa/1999/9912/oecdguide.htm>.

F. The Enforcement Scheme.

The enforcement scheme laid out by S. 630 likely would work well. It is modeled on similar schemes Congress established for enforcement for the Commission's 900-Number Rule and the Telemarketing Sales Rule in the statutes that mandated promulgation of those Rules.³³ The enforcement provisions would allow the Commission to treat violations of S. 630 as violations of a rule under Section 18 (15 U.S.C. § 57a) of the FTC Act regarding unfair or deceptive acts or practices. Moreover the Commission's efforts would be supplemented with those of the state Attorneys General, and possibly by other federal agencies with jurisdiction in areas where the FTC has none. This type of dual federal-state enforcement scheme has proved extremely successful in the past, particularly in challenging deceptive and abusive telemarketing practices, and the Commission would expect it to work equally well in this context.

G. The Effect on Other Laws [§ 7 of H.R. 630].

S. 630 provides an express savings clause for specific enforcement provisions of the Communications Act of 1934 and for federal criminal statutes. This express clause appears to preclude enforcement of most existing federal civil laws that apply to commercial electronic mail, such as the FTC Act's broad prohibition of deceptive advertising, except to the extent specifically provided in S. 630. The Commission believes that S. 630 should not supplant other relevant federal law, and recommends expanding the savings clause to make this clear.

*H. The Provision that Within 18 Months the Commission Conduct A Study of the Effectiveness and Enforcement of S. 630's Provisions.*³⁴

³³Telephone Disclosure and Dispute Resolution Act of 1992 (codified in relevant part at 15 U.S.C. §§ 5701 *et seq.*) and the Telemarketing and Consumer Fraud and Abuse Prevention Act (codified in relevant part at 15 U.S.C. §§ 6101-6108) .

³⁴The House bill, H.R. 718, contains a provision substantially similar to the mandatory study

(continued...)

A study of the effectiveness and enforcement of S. 630, if enacted with a requirement for such a study, would be based largely on the consumer complaint data from the Commission's UCE database. This database holds more than eight million UCE messages forwarded by consumers and providers of Internet access service. The Commission uses this database to assess the current state of UCE, spot emerging trends, and target its law enforcement efforts on the most serious problems. The Commission would be able to conduct a study on the effectiveness and enforcement of S. 630's provisions. However, 18 months may be too short a time frame for the Commission to effectively research and develop such a study. To meaningfully measure the effect of S. 630, it may be necessary to assess the situation before it goes into effect, and then gather data and information after it goes into effect and businesses have had time to come into compliance. The Commission therefore urges that the time frame for the study be extended to 24 months, in order to enhance the value of the study.

The Commission appreciates the opportunity to provide its views on S. 630 and on its efforts against deceptive UCE. I would be happy to answer any questions.

³⁴(...continued)
provision of S. 630.