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.

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 FTmf-2(s)]T4cas ch-14(et)-6 Tc 0.00(o)](2)2(T)-3(mf4(e m1(h)-4(6 Tc 0.00(ou m1(h)-4((t)-6TJ 0.0w)-2(or

advertising, industry 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 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 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

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.

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 bas

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 beees26(n 1996.)]TJ blas

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.

S. 630 includes a multi-faceted enforcement scheme. First, Section 5 of the Bill, described

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)].

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."[(29)] 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 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.[(30)] 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.[(31)] This could be accomplished by broadening the savings clause in Section 7(a) of the Bill.[(32)] Therefore, clarification of an intent to leave intact the Commission's 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.[33]

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

3. The FTC has limited or no jurisdiction over specified types of e(h)5(is)nt-3(d)-7(o)-7(rT.)-1(T)5(c)-3(ia-7(1 Tm [(-7(f)7(e7t Tm

12. A similar scheme that used spam was targeted in *FTC v. Lubell*, No. 3-96-CV