Testimony of Chris Murray, Legislative Counsel
Consumers Union

Before the

House Judiciary Committee,
Subcommittee on Crime, Terrorism, and Homeland Security

Regarding

H.R. 2214, the RID-SPAM Act

July 8, 2003

Subcommittee Chairman Coble, Ranking Member Scott, and other distinguished members of the Committee, thank you for the opportunity today to represent Consumers Union,[1] the print and online publisher of Consumer Reports, in your exploration of H.R. 2214, the "RID-SPAM Act" (sponsored by Reps. Burr, Sensenbrenner, and Tauzin).

It is almost unnecessary for me to detail what the problem with "spam"[2] is, because every time we open up our email inboxes we are confronted with exactly how bad things have gotten. When I arrive at work every morning, I can be confident that I will be greeted with at least a dozen messages advertising everything from life insurance and credit card offers to Viagra alternatives and pornography.

The ingenuity of spammers appears to be bottomless.[3] They find our addresses in novel ways. They have figured out myriad methods to avoid being filtered by Internet Service Providers (ISPs) and consumers. They have discovered how to commandeer our computers to send spam for them, and they are even finding new devices to spam us on. For example, text messaging on mobile phones, an increasingly popular application for consumers, is also becoming a haven for spam. While filtering technologies are becoming increasingly effective, unfortunately their efficacy is not increasing as fast as the volume of spam is growing.

Spam costs consumers and businesses money.

Some estimate that roughly 40% of all email is spam[4] and experts say that by the end of this year more than half of all email traffic will be spam. Consumers pay for all that spam, because when ISPs' costs go up—because ISPs have to buy more servers and pay personnel to figure out how to filter that spam—consumers' monthly ISP subscription fees go up.

One company estimates that spam will cost business $10 billion dollars this year alone (due to lost productivity, bandwidth costs, and money spent on filtering tools).[5] A

---

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports*, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* and *Consumer Reports Online* (with approximately 5 million paid circulation) regularly carry articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

[2] See Jonathan Krim, *"Protecting Its Proprietary Pork."* Washington Post, July 1, 2003 (E01). "Early Internet users coined the term spam to describe junk e-mail after a skit by the comedy group Monty Python. In the routine, a group of patrons at a restaurant chant the word "spam" in louder and louder volume, drowning out other conversation."

[3] See attached article, "E-Mail Spam: How to Stop It From Stalking You." Consumer Reports, August 2003.

[4] See Jonathan Krim, "Spam's Cost to Business Escalates." Washington Post, March 13, 2003 (A01).

[5] See www.ferris.com/rep/200301/SM.html.

study released last week estimates that spam costs businesses $874 per employee every year, because employees spend an average of 6.5 minutes every day dealing with it.[6]

America Online, the largest ISP, is currently blocking up to **2.4 billion** spam messages every day. [7] The costs of the bandwidth and servers required to move that volume of spam are astronomical—when we add the costs of sophisticated filtering systems and personnel to battle the continually escalating spam arms race, the costs of spam to ISPs (and ultimately to consumers) is truly staggering.

Recently the Washington Post reported that mainstream e-commerce companies are selling consumers email addresses to spammers.[8] For example, when consumers purchased popular "Hooked On Phonics" products, their addresses were being sold in complete violation of their privacy policy. That is, the company told consumers that they would not sell their personal information and then turned around and did precisely the opposite. "Hooked on Phonics'" corporate parent subsequently updated their privacy policy and said that they meant to update it earlier; they claimed they had done nothing wrong, they were simply slow to update their privacy policy.

Even worse, one company who was contracting with a 3rd party "shopping cart" provider (the mechanism used by consumers to complete an electronic commerce transaction) had a privacy policy which would have prevented consumers' email addresses from being shared with anyone. However, consumers might not have noticed that the shopping cart company behind the scenes of the electronic transaction—"Cart Manager"—had a completely different privacy policy and that by purchasing a product online, they were unwittingly making themselves vulnerable (there was no link to the shopping cart company's privacy policy in the process of check out).[9]

A relatively new practice, known as "email appending," raises enormous privacy concerns. Email appending is the practice of harvesting a consumer's email address from a Web site or other means and combining that consumer's email address with their mailing address, telephone number, and other personally identifiable information.

Mainstream companies such as Sears are using email appending to merge customers email addresses with their mailing addresses and their automotive repair histories. A marketing magazine recently told its readers how to "email append" their mailing lists:

> Send an Excel spreadsheet of your customers' names, addresses and phone numbers to an e-mail appending company, and the appending company will send back e-mail addresses that belong to those customers.

---

[6] "Spam: The Silent ROI Killer" by Nucleus Research. More information at: www.pcworld.com/news/article/0,aid,111433,00.asp.

[7] See testimony of Ted Leonsis (Vice Chairman and President, Advanced Products Group, America Online) before the Senate Commerce Committee, May 21, 2003.

[8] Jonathan Krim, "Web Firms Choose Profit Over Privacy." Washington Post, July 1, 2001 (A01).

[9] Id.

> What the appending company doesn't mention is that often it is missing a good deal of the information that you possess, and it may decide to append your data to its files just as it appends its e-mail addresses to yours. That means you are paying the company to incorporate your information into its e-mail database.
>
> For example, the automotive department at Sears provides its customers' names, addresses, phone numbers, and car models, makes and repair histories to e-mail appending firms when it requests customers' e-mail addresses. Sure, the company gets the e-mail addresses, but at the same time it contributes to privacy erosion -- all so it can send an e-mail about its lube, oil and filter change special.[10]

A large percentage of spam is also fraudulent and/or misleading, making it a serious consumer problem as well as difficult to prosecute. The Federal Trade Commission (FTC) recently issued a report[11] regarding false claims in spam, which found that 96% of spam had false information in either the message text or in the "From" and "Subject" lines.

Clearly, spam is ripe for legislative action. We agree with the ISPs and others that strong criminal enforcement and an ISP right of action are essential ingredients to successfully reducing spam. But thus far the bills proposed, including H.R. 2214, have an "opt-out" of spam as part of their core solution. In other words, an ISP must first pass on the spam to consumers, consumers must then read the spam, and then they can exercise their right to stop receiving messages from that particular sender (perhaps at their peril as described below). We believe H.R. 2214 needs to be improved because it lacks an "opt-in" provision and private right of action for consumers at the same time that it excludes class action suits. This puts too much burden on consumers to block spam and makes it too difficult to hold spammers legally accountable for their inappropriate interference with consumers' email.

Imagine that you put a "do not solicit" sign at the front door of your home, and every company in the world could only ring your doorbell once, at which point you would have the option to tell that salesperson that you did not want to be contacted anymore. Of course, in addition to telling that salesperson you didn't want to be solicited, you would have to do the same for solicitors that work for a different branch of the same company. You would need to keep track of each company you told not to solicit you, and if a company violated your request, you could petition the Federal Trade Commission to take up your case.

Of course, this is an absurd burden to place on people. We all know that "do not solicit" means exactly that. Consumers can say no to advertising at their front door, period. The Federal Trade Commission's recent enactment of a robust "do not call" list

---

[10] See Mike Banks Valentine, "E-Mail Appending Erodes Privacy." CRM Buyer Magazine, May 23, 2002. www.crmbuyer.com/perl/story/17914.html.

[11] www.ftc.gov/reports/spam/030429spamreport.pdf

means that now consumers have a tool to say no advertising at the dinner table. It is now incumbent on Congress to provide consumers with a tool to say no to advertising on our computers.

When the Federal Trade Commission recently took a close look at spam and what could be done to reduce it, many, if not most of the participants in that workshop agreed that opt-in was the best way to eliminate spam. It would be unwise for Congress to proceed down the opt-out path, which was clearly disfavored by experts.

Senate Judiciary Committee Chairman Hatch suggested several weeks ago that he would be willing to consider drafting legislation that entails an opt-in approach. He noted that one of the primary weaknesses of opt-out is that it leaves the burden on the consumer to eliminate spam. "People who receive dozens, even hundreds, of unwanted emails each day would have little time or energy for anything other than opting-out from unwanted spam."[12]

Senator Hatch continued on to say that,

> "[a] third way of attacking spam – and one that was favored by many panelists and audience members at the FTC forum – is to establish an opt-in system, whereby bulk commercial email may only be sent to individuals and businesses who have invited or consented to it. This approach has strong precedent in the Telephone Consumer Protection Act of 1991 (TCPA), which Congress passed to eliminate similar cost-shifting, interference, and privacy problems associated with unsolicited commercial faxes. The TCPA's ban on faxes containing unsolicited advertisements has withstood First Amendment challenges in the courts, and was adopted by the European Union in July 2002."[13]

As Senator Hatch points out, the Telephone Consumer Protection Act (also known as the "Junk Fax" law) could serve as a good model for dealing with spam. That law successfully helped eliminate junk faxing by 1) establishing an opt-in regime and 2) preserving a private right of action against violators, especially by allowing for the possibility of class action enforcement. We believe that the threat of class action enforcement combined with an opt-in approach is the best way to reduce spam for consumers.

In addition, Congress should not allow ISPs to be the primary entities driving a legislative solution. ISPs are an integral part of any solution, as their technical expertise and participation in enforcement is essential, but they have mixed incentives with regard to spam.

ISPs have clear incentives to reduce some amount of spam, because it costs them an enormous amount of money—except where the ISP is also a marketer. In the case of

---

[12] Senator Orrin Hatch and Senator Patrick Leahy Press Release, "*Hatch, Leahy Target Most Egregious Computer Spammers.*" Jun. 18, 2003.
[13] Id.

AOL and Microsoft, the two largest ISPs, those companies have clear incentives to get rid of other people's spam, but not such clear incentives to have limitations on their own spam. In fact, it may be that the best way for AOL and Microsoft to maximize their marketing revenues is to get rid of everyone's spam but their own, so that they can charge would-be spammers for preferred placement of spam. As the Washington Post recently reported, California state legislators were recently pressured by these companies as they tried to beef up spam regulations:

> One [California] state senator, who represents several Los Angeles suburbs, accused Microsoft of eleventh-hour arm-twisting to exempt Internet service providers from responsibility for being the conduits of spam. Firms such as Microsoft, America Online and Yahoo Inc. market to their own members, and large portions of overall e-mail traffic traverse their systems.
>
> "Microsoft is talking out of both sides of its mouth," said state Sen. Debra Bowen (D), who points to statements by Microsoft Chairman Bill Gates about how much the company is fighting to eliminate junk e-mail. But "their focus has been on getting immunity for themselves and preserving their ability to strike deals to send spam," she said.[14]

Ronald Scelson, also known as the "Cajun Spammer," testified before the Senate Commerce Committee[15] that some ISPs are signing "pink contracts" which allow spammers to send emails to ISPs' subscribers, charging the spammers more than they charge other commercial clients.

If these allegations are true, then it is unwise for Congress to give ISPs consumers' proxy on spam by allowing ISPs to have a right of action against spammers at the exclusion of individual suits and class actions. Giving ISPs a right of action will certainly help those ISPs to maximize the revenues they receive from spammers by providing them with a very large stick for spammers that do not pay, but it does not appear to be the best way to reduce spam.

Until Congress enacts meaningful legislation to fix the spam problem, Consumer Reports recommends that consumers deal with spam by doing nothing. This means do not respond to spam, do not view spam, and most especially, do not opt-out of spam because this will tell spammers that your email address is a functioning one.

This recommendation—that consumers do nothing with spam, and especially do not opt-out—is at obvious odds with bills that provide for opt-out as their way to clean up spam. That is because when consumers opt-out they are verifying for a spammer that their email addresses are current. Under an opt-out law, consumers would ostensibly have a remedy with spammers within the United States (i.e. spammers using opt-out for illegitimate purposes such as verifying that an email address is current could be prosecuted), but the opt-out law would still not apply for any spam originating outside the

---

[14] Jonathan Krim, "Internet Providers Battling to Shape Legislation: Microsoft, Others, Said to Want Immunity." Washington Post, July 5, 2003 (D10).
[15] Testimony of Ronald Scelson before the Senate Commerce Committee, May 21, 2003.

U.S.—spammers in other countries or offshore could not be prosecuted. Furthermore, it would be extremely difficult for consumers to tell whether email is originating from the U.S. or elsewhere.

In other words, once an opt-out spam bill were enacted into law, because of the continued possibility of cross-border fraud, we would still recommend to consumers that they should not exercise the opt-out—leaving consumers no better off than they are today.

In our August issue of Consumer Reports, we recommend the following 8 ways to block spam:

1. Don't buy anything promoted in spam. Even if the offer isn't a scam, you are helping to finance spam.
2. If your email address has a "preview pane," disable it to prevent the spam from reporting to its sender that you've received it.
3. Use one email address for family and friends, another for everyone else. Or pick up a free one from Hotmail, Yahoo!, or a disposable forwarding-address service like www.SpamMotel.com. When an address attracts too much spam, abandon it for a new one.
4. Use a provider that filters email, such as AOL, Earthlink, or MSN. If you get lots of spam, your ISP may not be filtering effectively. Find out its filtering features and compare them with competitors'.
5. Report spam to your ISP. To help the FTC control spam, forward it to uce@ftc.gov. ("uce" stands for unsolicited commercial email).
6. If you receive spam that promotes a brand, complain to the company behind the brand by postal mail, which makes more of a statement than email.
7. If your email program offers "rules" or "filters," use one to spot messages whose header contains one of more of these terms: html, text/html, multipart/alternative, or multipart/mixed. This can catch most spam, but may also catch most of the legitimate emails that are formatted to look like a Web page.
8. Install a firewall if you have broadband so a spammer can't plant software on your computer to turn it into a spamming machine. An unsecured computer can be especially attractive to spammers.

As mentioned earlier, as a legislative remedy, an opt-in regime (with a private right of action) appears to be the best choice. We recommend that consumers not opt-out of spam because this will simply confirm for the spammer that their email address is a live one. Opting out means getting more spam.

If we put ourselves in the shoes of a consumer trying to opt-out from spam several years from now, imagine trying to tell the difference between spam that is from a legitimate marketer, spam that originated from an overseas or offshore server, and spam that is simply a ripoff. There is no way I can think of under an opt-out regime to differentiate between these different types of spam. Opt-out may turn out to be a cop out.

It may be that there is a possibility for a modified version of opt-out, such as opt-out that allows for an entire domain to opt-out (e.g. "aol.com" could opt-out for all its users, so that individual users, such as "jane_doe@aol.com" do not have to give their names to spammers). This is one potential implementation of the "national do not spam" registry proposed by Senator Schumer. I have some misgivings about a "national do not spam" registry because of the obvious security risks posed by such a list, but I wonder if allowing entire domains to opt-out obviates some of those potential risks.

In addition, by including preemption of state laws and class actions, I believe HR 2214 will fail to stem the rising tide of spam. Congress should enact federal legislation that offers basic protection for consumers, and states should have a right to increase such protections based on unique local needs, just as the FTC did with the Federal "Do Not Call" list.

Any solution in the end will need to involve a variety of methods and actors, including a legislative remedy (opt-in with both private and ISP rights of action in addition to criminal enforcement), action from industry to improve filtering technologies as well as a way to attack the problem across international borders. It will be critical that Congress address the immense volume of fraud in spam, but Congress should also consider measures that will address mainstream companies' use of spam. While fraud is a huge problem, consumers' annoyance with spam does not end with rogue spammers. Just as the FTC's national "do not call" list allowed consumers to say no to advertising at the dinner table, consumers should have the ability to say no to all spam, even when that spam comes from companies that are not engaged in fraud.